

ALMOST CYCLIC ELEMENTS IN WEIL REPRESENTATIONS OF FINITE CLASSICAL GROUPS

LINO DI MARTINO AND A.E. ZALESSKI

Dedicated to Otto H. Kegel on the occasion of his 80th birthday

Abstract. This paper is a significant part of a general project aimed to classify all irreducible representations of finite quasi-simple groups over an algebraically closed field, in which the image of at least one element is represented by an almost cyclic matrix (that is, a square matrix M of size n over a field F with the property that there exists $\alpha \in F$ such that M is similar to $\text{diag}(\alpha \cdot \text{Id}_k, M_1)$, where M_1 is cyclic and $0 \leq k \leq n$). The paper focuses on the Weil representations of finite classical groups, as there is strong evidence that these representations play a key role in the general picture.

1. INTRODUCTION

Let V be a vector space of finite dimension n over an arbitrary field F , and let M be a square matrix of size n over F . Then M is said to be cyclic if the characteristic polynomial and the minimum polynomial of M coincide. Note that a matrix $M \in \text{Mat}(n, F)$ is cyclic if and only if the $F\langle M \rangle$ -module V is cyclic, that is, is generated by a single element. This is standard terminology in module theory, and the source of the term ‘cyclic matrix’. Matrices with simple spectrum often arising in applications are cyclic. We consider a generalization of the notion of cyclic matrix, namely, we define a matrix $M \in \text{Mat}(n, F)$ to be almost cyclic if there exists $\alpha \in F$ such that M is similar to $\text{diag}(\alpha \cdot \text{Id}_k, M_1)$, where M_1 is cyclic and $0 \leq k \leq n$.

Examples of almost cyclic matrices arise naturally in the study of matrix groups over finite fields. For instance, if an element $g \in GL(V)$ acts irreducibly on V/V' , where V' is some eigenspace of g on V , then g is almost cyclic. Reflections and transvections are important examples. Other relevant examples are provided by unipotent matrices with Jordan form consisting of a single non-trivial block.

Possibly, the strongest motivation to study groups containing an almost cyclic matrix is to contribute to the recognition of linear groups and finite group representations by the property of a single matrix. Our main inspiration is a paper by Guralnick, Penttila, Praeger and Saxl [19], in which the authors classified irreducible linear groups over finite fields generated by ‘Dempwolff elements’. If $V = V(n, q)$ is an n -dimensional vector space over a finite field of order q , and $G = GL(V) = GL(n, q)$, we say that $g \in G$ is a Dempwolff element if $|g| = p$ for some prime p with $(p, q) = 1$ and g acts irreducibly on $V^g := (\text{Id} - g)V$. U. Dempwolff in [6] initiated the study of subgroups of $GL(n, q)$ generated by such elements, obtaining a number of valuable results. The main restriction in [6] is the assumption that $2 \dim V^g > \dim V$, and this assumption is held in [19]. Clearly, Dempwolff elements are almost cyclic (and are reflections if $p = 2$). We have realized that, if one wishes to drop this restriction, and furthermore obtain satisfactory results in full generality, a more conceptual approach is available. Namely, one should deal with finite linear groups over an algebraically closed field. Therefore, our general program can be stated as follows: determine all irreducible finite linear groups over an algebraically closed field, which are generated by almost cyclic matrices. In addition, we wish to relax the assumption, held in [19], that g is of prime order. However, as current applications seem to

focus on p -elements, we will limit ourselves to the study of elements $g \in G$ of any p -power order.

Since we will make a systematic use of representation theory and will exploit the classification theorem of finite simple groups, a key part of our project necessarily focuses on finite quasi-simple groups. The sporadic simple groups and their covering groups have been completely dealt with in [7]. In [10], we started to deal with finite groups of Lie type, and determined all the irreducible representations of a quasi-simple group of Lie type G over an algebraically closed field F of characteristic coprime to the defining characteristic of G , in which the image of at least one unipotent element g is represented by an almost cyclic matrix. The complementary case, when g is unipotent in G , and the characteristic of F is the defining characteristic of G , has been settled for classical groups by Suprunenko in [41]. This leaves open the case when G is an exceptional group of Lie type, as well as the general case when g is a semisimple element of prime-power order of G .

The present paper focuses on Weil representations of finite classical groups (an overview of these representations is given in Section 5.1). The reason to treat this case separately is that there is strong evidence that most examples of semisimple almost cyclic elements occur in Weil representations. Furthermore, the study of Weil representations requires a lot of analysis and technical background which justifies the choice of treating them in an independent paper. Besides, Weil representations play a very significant role in the representation theory of classical groups, and several features and properties of them have been the subject of intensive study in many recent papers. So, the present paper can also be viewed as a contribution to this research area.

Before stating the main result, a few more words are needed about the existing literature. Before Dempwolff's work in [6], important results related to our problem had already appeared in the literature.

Ch. Hering ([21], [22]) essentially classified the finite irreducible subgroups G of $GL(n, q)$ containing an irreducible element of prime order, provided G has a composition factor isomorphic to a group of Lie type (or an alternating group). Also, the finite irreducible linear groups generated by transvections, reflections and pseudo-reflections were classified by A. Wagner in [49, 48], Pollatsek [36], A.E. Zalesski and V.N. Serezhkin in [58, 59]. I.D. Suprunenko and A.E. Zalesski in [42, 43] classified the irreducible representations of Chevalley groups in the natural characteristic containing a matrix with simple spectrum. Furthermore, Di Martino and Zalesski in [8, 9], following an earlier paper by Zalesski [54], studied the minimum polynomials of elements of prime power order in the cross characteristic representations of classical groups. This was further extended by Tiep and Zalesski in [47]. The latter work also extends part of the results of [55, 56] to representations over fields of prime characteristic.

More information is available in the case where the ground field F is of characteristic zero. Huffman and Wales in [25] classified the finite irreducible linear groups generated by elements g such that $\dim V^g \leq 2$. As a particular case, this result contains a classification of finite irreducible linear groups over the complex numbers generated by almost cyclic elements of order 3. Zalesski in [55] determined the irreducible linear groups over the complex numbers generated by elements g of prime order $p > 3$ that have at most $p - 2$ distinct eigenvalues. In addition, in [56] Zalesski determined the irreducible representations of quasi-simple groups in which an element of prime order p has at most $p - 1$ distinct eigenvalues. Another relevant work for the characteristic 0 case is [37]. See also the surveys [46, 57] for further details.

Now, we state our main result.

Theorem 1.1. *Let G be one of the following groups: $G = Sp(2n, q)$, where $n > 1$ and q is odd; $SU(n, q) \subseteq G \subseteq U(n, q)$, where $n > 2$; $SL(n, q) \subseteq G \subseteq GL(n, q)$, where $n > 2$. Let $g \in G$ be a non-scalar p -element, where p is a prime not dividing q . Let F be an*

algebraically closed field of characteristic ℓ not dividing q , and τ an irreducible Weil F -representation of G . Then the matrix of $\tau(g)$ is almost cyclic if and only if one of the following occurs:

- (1) $G = Sp(2n, q)$, and either
 - (a) n is a 2-power and $|g| = (q^n + 1)/2$ is odd, or
 - (b) $q = 3$, $n \neq p$ is an odd prime, and $|g| = (3^n - 1)/2$ is odd, or
 - (c) $n = 2$, $q = 3$, and one of the following holds:
 - (c₁) $p = 2$, $\ell \neq 2$ and either $|g| = 2$ and $\dim \tau = 5$, or $|g| = 4$, $g^2 \notin Z(G)$ and $\dim \tau = 4$, or $|g| = 8$, $g^4 \in Z(G)$ and $\dim \tau = 4$ or 5 ;
 - (c₂) $p = 5$ and $\dim \tau \in \{4, 5\}$, where $\dim \tau \neq 5$ if $\ell = 2$;
 - (c₃) $p = \ell = 2$ and $\dim \tau = 4$. In addition, either $|g| = 4$ or $|g| = 2$.
- (2) $SU(n, q) \subseteq G \subseteq U(n, q)$, and either
 - (a) $|g| = (q^n + 1)/(q + 1)$ and $n \neq p$ is an odd prime greater than 3, or
 - (b) $(n, q) = (5, 2)$, $|g| = 9$, $\ell \neq 3$ and $\dim \tau = 10$;
 - (c) $(n, q) = (4, 2)$ and one of the following holds:
 - (c₁) $|g| = 3$ or 9 ;
 - (c₂) $|g| = 5$; or
 - (d) $(n, q) = (3, 3)$, and one of the following holds:
 - (d₁) $|g| = 7$;
 - (d₂) $|g| = 8$ and either $\dim \tau = 6$, or $\ell \neq 2$ and $\dim \tau = 7$; or
 - (e) $(n, q) = (3, 2)$, $|g| = 3$ or 9 and $\dim \tau = 2, 3$ for $\ell \neq 2$, $\dim \tau = 3$ for $\ell = 2$.
- (3) $SL(n, q) \subseteq G \subseteq GL(n, q)$, and either
 - (a) $G = SL(n, 2)$, where $n \neq p$ is an odd prime and $|g| = 2^n - 1$ is a Mersenne prime, or
 - (b) $|g| = (q^n - 1)/(q - 1)$, where $q > 2$, and $n \neq p$ is an odd prime.

For the sake of completeness we have also examined in this paper the case where $SL(2, q) \subseteq G \subseteq GL(2, q)$, without assuming that τ is Weil. Note that the degree of an irreducible F -representation of G in this case belongs to the set $\{1, q - 1, q, q + 1, (q - 1)/2, (q + 1)/2\}$, where in the last two cases q is odd.

The results obtained are collected in Theorem 1.2 below. Additionally, these results (as a consequence of Lemma 4.9 and Corollary 4.10 in Section 4) can be carried over to any group G such that $SU(2, q) \subseteq G \subseteq U(2, q)$.

Theorem 1.2. *Let $SL(2, q) \subseteq G \subseteq GL(2, q)$, $q > 3$, and let $g \in G$ be a non-scalar p -element, where p is a prime not dividing q . Let F be an algebraically closed field of characteristic ℓ not dividing q , and let M be an irreducible FG -module with $\dim M > 1$, affording the representation τ . The following holds:*

(1) *Suppose $p > 2$. Then $\tau(g)$ is almost cyclic if and only if $\dim M \leq |g| + 1$. (In this case, $(2, q + 1)|g| = q \pm 1$).*

(2) *Suppose $p = 2$, and let h denote the projection of g into $G/Z(G)$.*

Assume first that $q \equiv 1 \pmod{4}$. Then $\tau(g)$ is almost cyclic if and only if one of the following occurs:

- (i) $\ell \neq 2$, $g \in SL(2, q) \cdot Z(GL(2, q))$, $\dim M = (q \pm 1)/2$ and $|h| = (q - 1)/2$;
- (ii) $\ell \neq 2$, $g \notin SL(2, q) \cdot Z(GL(2, q))$, and either $\dim M = q$ or $q - 1$ and $|h| = q - 1$, or $G = GL(2, 5) \cong \tau(G)$, $\dim M = 4$, $|g| = 8$ and $|h| = 2$;
- (iii) $\ell = 2$ and either $\dim M \leq |h| + 1$ or $G = GL(2, 5)$, $\tau(G) \cong O^-(4, 2)$, $\dim M = 4$ and $\tau(g)$ is a transvection.

Next, assume that $q \equiv -1 \pmod{4}$.

Then $\tau(g)$ is almost cyclic if and only if one of the following occurs:

- (i) $\ell \neq 2$, $g \in SL(2, q) \cdot Z(GL(2, q))$, $\dim M = (q \pm 1)/2$ and $|h| = (q + 1)/2$;
- (ii) $\ell \neq 2$, $g \notin SL(2, q) \cdot Z(GL(2, q))$, $\dim M = q$ or $q \pm 1$ and $|h| = q + 1$;
- (iii) $\ell = 2$, and one of the following holds:

- a) $\dim M = q \pm 1$ and $|h| = q + 1$ (here the case $\dim M = q + 1$ only occurs for $g \notin SL(2, q) \cdot Z(GL(2, q))$);
- b) $\dim M = (q - 1)/2$ and $|h| = (q + 1)/2$;
- c) $q = 7$, $\dim M = 3$ and $|h| = 2$.

NOTATION

Throughout the paper, unless stated otherwise, we denote by F an algebraically closed field of characteristic ℓ .

For any finite group G , the representations of G we consider in the paper are all over F , unless stated otherwise. We write 1_G for the trivial FG -module and ρ_G^{reg} for the regular FG -module (that is the free FG -module of rank 1).

If G is a finite group of Lie type of defining characteristic r , we always assume that ℓ is coprime to r .

For the reader's sake, it is also convenient to lay down explicitly some of the notation which is used throughout the paper for finite classical groups.

Let V be a vector space of finite dimension $m > 1$ over a field K .

If K is a finite field of order q (where q is a power of a prime r), K will be usually denoted by \mathbb{F}_q , and the general linear group $GL(V)$ and the special linear group $SL(V)$ will be denoted by $GL(m, q)$ and $SL(m, q)$, respectively.

Suppose that the space V is endowed with a non-degenerate orthogonal, symplectic or unitary form. Then $I(V)$ will denote the group of the isometries of V , and we will loosely use the term 'finite classical group' for a subgroup G of $I(V)$ containing $I(V)'$. In particular: if V is a symplectic space over \mathbb{F}_q , $I(V)$ will be denoted by $Sp(m, q)$; if V is a unitary space over the field \mathbb{F}_{q^2} , $I(V)$ will be denoted by $U(m, q)$; and if V is an orthogonal space over \mathbb{F}_q , $I(V)$ will be denoted by $O(m, q)$. It should be noted that in places the term 'classical group' will be meant to include also the groups $GL(m, q)$ and $SL(m, q)$ (considering V endowed with the identically zero bilinear form). Finally, at times we will need to consider, for a given classical group G (defined as above) the corresponding central quotient (projective image), which will be denoted by PG .

Finally, we mention that the notation used in the paper for objects of general group theory is fairly standard. E.g., for a group G , $Z(G)$ denotes the centre of G ; for a subgroup H of G , $N_G(H)$ and $C_G(H)$ denote the normalizer and the centralizer of H in G , respectively. Similarly, for $x \in G$, $C_G(x)$ denotes the centralizer of x in G . And so on.

2. PRELIMINARIES

For the reader's convenience we recall the following definition:

Definition 2.1. *Let M be an $(n \times n)$ -matrix over an arbitrary field K . We say that M is almost cyclic if there exists $\alpha \in K$ such that M is similar to $\text{diag}(\alpha \cdot \text{Id}_k, M_1)$, where M_1 is cyclic and $0 \leq k \leq n$.*

Remark 1. In the definition above, it has to be understood that for $k = 0$ the matrix $M = M_1$ is cyclic, whereas for $k = n$ the matrix M is scalar.

Remark 2. Let \overline{K} denote the algebraic closure of K , and for $\lambda \in \overline{K}$ denote by λJ a Jordan block with eigenvalue λ . Observe that a matrix M_1 is cyclic if and only if M_1 has Jordan form $\text{diag}(\lambda_1 J_1, \dots, \lambda_s J_s)$, where the λ_j 's, $1 \leq j \leq s$, are pairwise distinct. In particular, suppose that M has order p^a , where p is a prime, and set $\ell = \text{char } K$. Then M is almost cyclic if and only if the eigenvalues of M_1 in \overline{K} are pairwise distinct when $\ell \neq p$, and if and only if M_1 consists of a single Jordan block when $\ell = p$.

An elementary observation, which will be useful throughout the paper, is the following: if $M \in GL(V)$ is almost cyclic, and U is an M -stable subspace of V , then the induced action of M on U and on V/U yield almost cyclic matrices.

Let us denote by $\deg(X)$ the degree of the minimum polynomial of a square matrix X over a field F . Then the following holds:

Lemma 2.2. *Let A, B be non-scalar square matrices over an arbitrary field K , both diagonalizable over K , and let $k = \deg(A), l = \deg(B)$. Suppose that $A \otimes B$ is almost cyclic. Then A, B are cyclic and $\deg(A \otimes B) \geq kl - \min\{k, l\} + 1$.*

Proof. The claim about the cyclicity of A and B is obvious. Assume $k \leq l$ and let $\varepsilon_1, \dots, \varepsilon_k, \eta_1, \dots, \eta_l$ be the eigenvalues of A, B , respectively. If $A \otimes B$ is cyclic, then $\deg(A \otimes B) = kl$. Suppose $A \otimes B$ is not cyclic. We can assume that $\lambda = \varepsilon_1 \eta_1$ is an eigenvalue of $A \otimes B$ of multiplicity greater than 1. Then all the $\varepsilon_i \eta_j$'s such that $\varepsilon_i \eta_j \neq \lambda$ are distinct. The number of pairs (i, j) such that $\varepsilon_i \eta_j = \lambda$ is at most k , and hence $A \otimes B$ has at least $1 + (kl - k)$ distinct eigenvalues, as required.

Remark. A typical application of Lemma 2.2 is the following. Let $X = X_1 \times X_2$ be the direct product of two groups X_1, X_2 and $g \in X$ be a p -element for some prime p . Then $g = g_1 g_2$, where $g_1 \in X_1, g_2 \in X_2$. Let $\phi \in \text{Irr}_F X$, where F is an algebraically closed field of characteristic different from p . Then $\phi = \phi_1 \otimes \phi_2$, where $\phi_i \in \text{Irr } X_i$ for $i = 1, 2$. Suppose that $\phi_i(g_i)$ has order $p^{m_i} > 1$ modulo the scalars, and let $\phi_i(g_i^{p^{m_i}}) = \lambda_i \cdot \text{Id}$ for some $\lambda_i \in F$. We may assume $m_1 \geq m_2$. Clearly, every eigenvalue of $\phi_i(g_i)$ is a p^{m_i} -root of λ_i . Furthermore, we have $\phi(g) = \phi_1(g_1) \otimes \phi_2(g_2)$. It follows that the eigenvalues of $\phi(g)$ are p^{m_1} -roots of $\lambda_1 \lambda_2^{p^{m_1-m_2}}$, and the minimum polynomial of $\phi(g)$ is of degree at most p^{m_1} . Lemma 2.2 tells us that if k, l are the degrees of the minimum polynomials of $A = \phi_1(g_1)$ and $B = \phi_2(g_2)$, respectively, then $\phi(g)$ is not almost cyclic unless (a) A, B are cyclic matrices and (b) $p^{m_1} \geq kl - \min\{k, l\} + 1$.

Lemma 2.3. *Let λ, μ be two completely reducible representations of a cyclic p -group $X = \langle x \rangle$ of order p^a over a field K , and let l and k , where $l \geq k > 1$, be the degrees of the minimum polynomials of $\lambda(x), \mu(x)$, respectively. Suppose that $k + l > p^a > 3$. Then $\lambda(x) \otimes \mu(x)$ is not almost cyclic.*

Proof. Suppose the contrary. Then, by Lemma 2.2, $p^a \geq \deg(\lambda(x) \otimes \mu(x)) \geq k(l-1) + 1$. As $k + l > p^a$, we have $l \geq \frac{p^a+1}{2}$. So $p^a \geq k(\frac{p^a+1}{2} - 1) + 1 = k(\frac{p^a-1}{2}) + 1 = p^a + (k-2)\frac{p^a-1}{2}$, whence $k = 2$. This implies $2 + l > p^a \geq 2l - 1$, whence $2 + l > 2l - 1$, that is $l = 2$. This in turn forces $p^a < 4$. A contradiction, as $p^a > 3$ by assumption.

Lemma 2.4. *Let K be a field of arbitrary characteristic ℓ , and let J_m, J_n be unipotent Jordan blocks of size $m \geq n > 1$ over K . Then $J_m \otimes J_n$ is almost cyclic if and only if $m = n = 2$ and $\ell \neq 2$.*

In particular, if $\ell > 0$, $P = \langle g \rangle$ is a cyclic ℓ -group, and M, N are non-trivial indecomposable KP -modules, then the matrix of g on $M \otimes N$ is almost cyclic if and only if M and N are of dimension 2 and $\ell \neq 2$.

Proof. Let V_m and V_n be vector spaces over K on which J_m and J_n act, respectively. Clearly, for every $1 \leq i \leq m$ there is exactly one subspace V_i of dimension i in V_m , which is stable under J_m . Similarly, for every $1 \leq j \leq n$ there is a single subspace V_j of V_n stable under J_n . Moreover, each V_i is indecomposable under the action of J_m . Similarly for each V_j . Now, $J_m \otimes J_n$ acts on $V_m \otimes V_n$, and stabilizes each subspace $V_i \otimes V_j$. In order to prove the first part of the statement, it is enough to prove that $J_m \otimes J_n$ is almost cyclic if $m = n = 2$ and $\ell \neq 2$, whereas it is not almost cyclic if $m = 3, n = 2$ or $n = m = \ell = 2$.

A direct computation shows that, if $m = n = 2$, then $V_2 \otimes V_2 = W_1 \oplus W_2$, where W_1, W_2 are $(J_m \otimes J_n)$ -stable subspaces and $\dim W_1 = \dim W_2 = 2$ if $\ell = 2$, whereas $\dim W_1 = 3$ and $\dim W_2 = 1$ if $\ell \neq 2$.

Next, let $m = 3, n = 2$. In this case we do not need to consider $\ell = 2$. A direct computation shows that $V_3 \otimes V_2 = W_1 \oplus W_2$, where W_1, W_2 are $(J_m \otimes J_n)$ -stable subspaces, and $\dim W_1 = \dim W_2 = 3$ if $\ell = 3$, whereas $\dim W_1 = 4$ and $\dim W_2 = 2$ if $\ell \neq 3$.

The additional claim of the lemma is a module-theoretic version that follows straightforwardly from the first part.

Lemma 2.5. *Let $T = RH$ be a finite group where $H = \langle h \rangle$ is a cyclic p -subgroup and R is a normal r -subgroup for some prime $r \neq p$. Let $|H/C_H(R)| = p^k$. Let ϕ be an F -representation of T faithful on R . Suppose that $(\ell, r) = 1$ and $1 < \deg \phi(h) < m(h)$ where $m(h)$ is the order of h modulo $Z(H)$. Then R is non-abelian and $p^a = r^b + 1$ for some $a, b \in \mathbb{N}$. Additionally, $\deg \phi(h) \geq (p^a - 1)p^{k-a}$.*

For $\ell = p > 0$ the proof can be found, for instance, in [15, VII.10.2]. Observe that a faithful $\mathbb{C}R$ -module remains faithful under reduction modulo p , and the degree of the minimum polynomial cannot increase. So Lemma 2.5 is valid for characteristic 0. Using reduction modulo $\ell \neq r$, one obtains the result for $\ell \neq p$, as the character of H coincides on ℓ' -elements with the Brauer character.

Lemma 2.6. [28, Ch. IX, Lemma 2.7] *Let p, r be primes and a, b positive integers such that $p^a = r^b + 1$. Then either $p = 2, b = 1$, or $r = 2, a = 1$ or $p^a = 9$.*

Recall that an element g of a group of Lie type G of defining characteristic ℓ is said to be semisimple if g has order coprime to ℓ . Furthermore, we will say that g is regular semisimple if its centralizer in G has order coprime to ℓ (this definition, convenient in our context, is well-known to be equivalent to that usually given in the context of algebraic groups).

The series of results that follow will be crucial for our purposes.

Lemma 2.7. (Gow [17]) *Let G be a quasi-simple group of Lie type in characteristic r and $g \in G$. Suppose that $(|C_G(g)|, r) = 1$, that is, $C_G(g)$ contains no element of order r . Then every semisimple element of G can be factorized as ab , where $a, b \in g^G$.*

Lemma 2.8. *Let G be a quasi-simple group of Lie type. Then the following holds:*

- (1) *G can be generated by two semisimple elements.*
- (2) *Let $g \in G$ be a regular semisimple element. Then G can be generated by three elements conjugate to g .*

Proof. (1) Obviously, it suffices to prove the statement for G simple. Let r be the defining characteristic for G . If $r = 2$, then the result is available from [18, Theorem 8.1]. So, let $r > 2$. If G is classical or of type $E_6, {}^2E_6(q)$, then the result is contained in the proof of Theorem 3.1 in [35], except for groups $\Omega^\pm(8, 2)$ (which are covered by [18]) and the group $PSU(3, 3)$. (Note that the case of the groups of type $A_1(q)$ goes back to L.E. Dickson.) The group $PSU(3, 3)$ is easily dealt with: it is generated by an elements of order 7 and 4 (from the class 4A in [5]). Furthermore, it is shown in [32] that the groups $G \in \{F_4(q), E_6(q), {}^2E_6(q), E_7(q), E_8(q)\}$ are generated by a pair of elements x, y with $x^2 = y^3 = 1$ (this is called a $(2, 3)$ -generation). Therefore, if $(6, q) = 1$, we are done. If $r = 3$, the result for these groups again follows from [32], where a $(2, 3)$ -generation is provided, with the additional property that $c = xy$ is a semisimple element of a suitable kind. Clearly, $G = \langle x, c \rangle$, and x, c are semisimple. The groups $G \in \{G_2(q), {}^2G_2(q), {}^3D_4(q)\}$ for q odd are known to be $(2, 3, 7)$ -generated (that is, they are generated by two elements x and y of order 2 and 3, respectively, such that xy has order 7), with the exception of the groups ${}^2G_2(3), G_2(3), {}^3D_4(3^n)$ (see [33], [34]). So the result follows as above, apart for the quoted exceptions. The groups $G_2(3), {}^3D_4(3^n)$ are covered in [33] (see the proof of the Corollary, p. 350) and in [34] (see the proof of Proposition 3), respectively. Finally the simple group ${}^2G_2(3)'$ is isomorphic to $SL(2, 8)$, and hence the result follows.

(2) By (1), every quasi-simple group of Lie type can be generated by two semisimple elements. Therefore, if $g \in G$ is regular semisimple, then, by Lemma 2.7, G can be generated by four elements conjugate to g . It was proven in [18] and [40] that for any non-trivial $g \in G$, there exists a suitable $h \in G$ such that $G = \langle g, h \rangle$, and furthermore that h can be chosen to be semisimple. It now follows from Lemma 2.7 that G can be generated by three conjugates of any given regular semisimple element g .

The following Propositions are due to R. Guralnick and J. Saxl ([20]).

Proposition 2.9. *Let G be simple group of Lie type, and let $1 \neq x \in \text{Aut}(G)$. Denote by $\alpha(x)$ the minimum number of G -conjugates of x sufficient to generate $\langle x, G \rangle$. Then the following holds:*

(1) ([20, Theorem 4.2]) *Let G be a simple classical group, and assume that the natural module for G has dimension $n \geq 5$. Then $\alpha(x) \leq n$, unless $G = \text{PSp}(n, q)$ with q even, x is a transvection and $\alpha(x) = n + 1$.*

(2) ([20, Theorem 5.1]) *Let G be a simple exceptional group of Lie type, of untwisted Lie rank m . Then $\alpha(x) \leq m + 3$, except possibly for the case $G = F_4(q)$ with x an involution, where $\alpha(x) \leq 8$.*

In the same paper, the authors prove analogous results for low-dimensional classical groups. We quote the following, which will be needed in the sequel:

Proposition 2.10. *Under the same assumptions and notation of Proposition 2.9, the following holds:*

(1) ([20, Theorem 4.1(a)]) *If $G = \text{PSL}(3, q)$, and x has prime order, then $\alpha(x) \leq 3$, unless x is an involutory graph field automorphism with $\alpha(x) \leq 4$.*

(2) ([20, Theorem 4.1(c)]) *If $G = \text{PSL}(4, q)$, $q > 2$, and x has prime order, then $\alpha(x) \leq 4$, unless x is an involutory graph automorphism with $\alpha(x) \leq 6$.*

(3) ([20, Theorem 4.1(d)]) *If $G = \text{PSL}(4, 2)$, and x has prime order, then $\alpha(x) \leq 4$, unless x is a graph automorphism with $\alpha(x) = 7$.*

(4) ([20, Lemma 3.3]) *If $G = \text{PSU}(3, q)$, $q > 2$, and x has prime order, then $\alpha(x) \leq 3$, unless $q = 3$ and x is an inner involution with $\alpha(x) = 4$.*

(5) ([20, Lemma 3.4]) *If $G = \text{PSU}(4, q)$ and x has prime order, then $\alpha(x) \leq 4$, unless one of the following holds:*

- (i) *x is an involutory graph automorphism and $\alpha(x) \leq 6$;*
- (ii) *$q = 2$ with x a transvection and $\alpha(x) \leq 5$.*

(6) ([20, Theorem 4.1(f)]) *If $G = \text{PSp}(4, q)$ and x is of prime order, then $\alpha(x) \leq 4$, unless x is an involution and $\alpha(x) \leq 5$, or $q = 3$ and $\alpha(x) \leq 6$.*

The following result, which only requires elementary linear algebra, will often be applied in this paper in order to establish a connection between the occurrence of almost cyclic matrices in representations of irreducible linear groups and the generation of these groups by conjugates. In particular, it will be usually combined with Lemma 2.8 and Propositions 2.9 and 2.10.

Lemma 2.11. *If $G < \text{GL}(n, F)$ is a finite irreducible linear group generated by m almost cyclic elements of the same order d modulo $Z(G)$, then*

$$n \leq m(d - 1).$$

Proof. See ([7, Lemma 2.1]).

Furthermore, we quote the following result, which will be useful in the next sections.

Lemma 2.12. (see [36]) *Suppose that $\text{char} F = \ell = 2$. Let G be an irreducible subgroup of $\text{GL}(n, F)$ generated by transvections. Then G is isomorphic either to a symmetric group S_{n+1} or S_{n+2} , where n is even, or to one of the groups $\text{SL}(n, q)$, $\text{Sp}(n, q)$, $O^\pm(n, q)$, $\text{SU}(n, q)$, where q is a 2-power.*

We close this section by recording some results which follow from the representation theory of finite groups having cyclic Sylow p -subgroups for some prime p .

Lemma 2.13. *Let G be a finite group with a non-trivial cyclic ℓ -subgroup P of order ℓ^d , and let M be an irreducible FG -module faithful on P . Then the following holds:*

- (1) *if M is of defect zero, then $M|_P = \frac{\dim M}{|P|} \rho_P^{\text{reg}}$;*
- (2) *if M is of defect d , then $M|_P = \frac{\dim M - \dim L}{|P|} \rho_P^{\text{reg}} \oplus L$, where L is the direct sum of isomorphic indecomposable FP -modules of dimension $e < |P|$. In addition, if $N_G(P)/P$ is abelian, then $L|_P$ is indecomposable.*

Proof. Suppose first that M has defect zero. It is well known that $M|_P$ is a projective module, and hence a multiple of ρ_P^{reg} . Whence (1).

Next, suppose that M has defect d . Set $N = N_G(P)$. By [15, Lemma VII.1.5], $M|_N = L \oplus A_1 \oplus A_2$, where A_1 is projective, $A_2|_P$ is projective and L is the Green correspondent of M . Therefore, $(A_1 \oplus A_2)|_P$ is projective. As $P = \langle y \rangle$ is cyclic, every projective FP -module is free, so $(A_1 \oplus A_2)|_P = \frac{\dim M - \dim L}{|P|} \cdot \rho_P^{\text{reg}}$. Recall that L is indecomposable as an FN -module ([15, Theorem III.5.6]) and uniserial ([15, Theorem VII.2.4]), that is, the submodule lattice of L is a chain. Set $x = 1 - y$ in the group algebra FN , $L_0 = L$ and $L_i = x^i L$ for $i = 1, \dots, e$, assuming $L_e = 0$ and $L_{e-1} \neq 0$. Observe that L_1 is an FN -module (indeed, for $n \in N$ we have $nL_1 = (1 - nyn^{-1})L = (1 - y^j)L$ for some integer $j > 0$, and $1 - y^j = (1 - y) + (1 - y)y + \dots + (1 - y)y^{j-1}$). It follows that L_i is an FN -module for every i . As P acts trivially on every quotient L_i/L_{i+1} , the latter module is completely reducible, and hence irreducible, since L is uniserial, for every i . By [15, Theorem VII.2.4], all the composition factors of L are of the same dimension c , say. By the definition of the L_i 's, it follows that $L|_P$ is a direct sum of c copies of an indecomposable representation of P of dimension e , and $e = \dim L/c$. Note that $e < |P|$, as otherwise M would be of defect 0. In addition, if $N_G(P)/P$ is abelian, then $c = 1$. So the (2) follows.

Remark. Observe that, if G is a quasi-simple group of Lie type with a non-trivial cyclic ℓ -subgroup P of order ℓ^d , then P is a TI-subgroup (see [2], or [54, Lemma 3.3(ii)]). This implies that every irreducible FG -module is either of defect 0 or defect d , as the defect group is the intersection of two Sylow p -subgroups.

Corollary 2.14. *Let G, P, M be as in Lemma 2.13, with M of defect d , and let $1 \neq g \in P$. Suppose that g is almost cyclic on M . Then either $M = L$ and $\dim L < |P|$, or $M|_P = \rho_P^{\text{reg}} \oplus L$ and P is trivial on L . In the latter case, $\dim L = c$, where c is the dimension of an irreducible representation of $N_G(P)/P$; in particular, if $N_G(P)/P$ is abelian, then $\dim M = |P| + 1$.*

Proof. Obviously, g is almost cyclic on L . By Lemma 2.13, this implies that either $L|_P$ is indecomposable or $L|_P$ is trivial. In the former case, $\dim L < |P|$. Suppose $M \neq L$. Then $M = \rho_P^{\text{reg}} \oplus L$, and $L|_P$ is trivial. Observe (cfr. the proof of Lemma 2.13) that L is indecomposable as an $FN_G(P)$ -module; hence, as $L|_P$ is trivial, it is in fact an irreducible $F(N_G(P)/P)$ -module. It follows that $\dim L = c$. In particular, if $N_G(P)/P$ is abelian, then $\dim M = |P| + 1$.

3. GROUPS WITH A NORMAL SUBGROUP OF SYMPLECTIC TYPE

In this Section, we collect miscellaneous results concerning groups containing normal subgroups of 'symplectic type', with special focus on the occurrence of almost cyclic elements in representations of such groups, which will be essential in the sequel of the paper. In particular, some applications to primitive linear groups containing non-central solvable normal subgroups will be obtained (cfr. Lemma 3.9 and Theorem 3.10).

Let E be a finite r -group for a prime r . We recall that E is said to be 'of symplectic type' if it has no non-cyclic characteristic abelian subgroups. The structure of such groups is well understood (e.g. cf. [1, p.109]). [Namely, by an old result of Philip Hall, if E is a r -group of symplectic type, then E is the central product of subgroups A and R , where: 1) either A is extraspecial or $A = 1$, and 2) either R is cyclic or R is dihedral, semidihedral or quaternion, of order $\geq 2^4$.] Certain r -groups of symplectic type naturally appear in the

Clifford theory of linear groups as irreducible subgroups of primitive linear groups G over algebraically closed fields, when G has a non-central solvable normal subgroups. Namely, these r -groups either are extraspecial of order r^{1+2n} (of prime exponent r if r is odd, and of exponent 4 if $r = 2$) or they are 2-groups of order r^{2+2n} and exponent 4 (with cyclic centre of order 4 and derived subgroup of order 2). Their structure is fully described, e.g. in [30, p. 149, Table 4.6.A]. Their faithful irreducible representations over an algebraically closed field of characteristic $\ell \neq r$ are also well-known (e.g. cf. [44, p.335] and [30, pp. 149-150]). In particular, they are all of degree r^n . Moreover, they are uniquely determined by their restrictions to $Z(E)$, and their characters vanish outside $Z(E)$.

In the sequel of the paper, by ‘ r -group of symplectic type’ we always mean a group of the above kind (i.e. one of the groups listed in [30, Table 4.6.A]).

Remark. In [31] Landazuri and Seitz considered a class of r -groups, called ‘groups of extraspecial type’, which appear as unipotent radicals of certain parabolic subgroups of finite groups of Lie type. These groups are closely related to our ‘groups of symplectic type’. Namely, if G is a group of extraspecial type, for any subgroup Z_1 of index r in $Z(G)$ the quotient group G/Z_1 is a group of symplectic type with centre of order r .

Lemma 3.1. *Let G be a finite group containing a normal subgroup E , where E is an r -subgroup of symplectic type and $|E/Z(E)| = r^{2n}$. Suppose that $G = E \cdot S$, where $S = \langle g \rangle$ and $Z(E) \subseteq Z(G)$. Let M be an irreducible FG -module non-trivial on $Z(E)$. Then M is irreducible as FE -module and $\dim_F M = r^n$.*

Proof. See [28, Ch.IX, Lemma 2.5], where E is supposed to be extraspecial. However, the proof remains valid without changes for E of symplectic type.

Lemma 3.2. *Let G be a finite group containing a normal subgroup E , where E is an r -subgroup of symplectic type and $|E/Z(E)| = r^{2n}$. Suppose that $G = E \cdot S$, where $S = \langle g \rangle$, $Z(E) \subseteq Z(G)$, $C_S(E) = 1$. Suppose that $|g| = r^n - \varepsilon$, where $\varepsilon \in \{1, -1\}$. Suppose furthermore that E contains no g -invariant non-abelian subgroups. Let M be an irreducible FG -module faithful on E . Then the following holds:*

- (1) *If $\varepsilon = -1$, then $M|_S$ is isomorphic to a submodule of codimension 1 in ρ_S^{reg} and the matrix of g on M is cyclic.*
- (2) *If $\varepsilon = 1$, then:*
 - (i) *$M|_S \cong \rho_S^{\text{reg}} \oplus L$, where L is a 1-dimensional FS -module.*
 - (ii) *Suppose that $\ell = \text{char } F > 0$, and $P \neq 1$ is the Sylow ℓ -subgroup of S . Let $S = PB$, where $B = \langle b \rangle$ is an ℓ' -subgroup of S . Let U be a sum of some eigenspaces of b on M . Then the matrix of g on U is cyclic if and only if $\dim U \equiv 0 \pmod{\ell}$.*
 - (iii) *Let $1 \neq z \in P$. Then the matrix of g is cyclic on $(1 - z)M$.*

Proof. Set $V = E/Z(E)$. Then V is a non-degenerate symplectic space over F_r with respect to the bilinear form on V induced by the commutator map $(a, b) \rightarrow [a, b]$ ($a, b \in E$). Let h be the automorphism of V induced by the conjugation action of g . Then h can be viewed as an element of the symplectic group $Sp(2n, r)$. Note that $|h| = |g| = r^n - \varepsilon$, as $C_S(E) = 1$.

Let $t \neq 1$ be a power of h . Then t acts fixed-point freely on $V \setminus \{0\}$. Indeed, let V^t be the fixed point subspace of t on V ; it is well known that V^t is non-degenerate, as t is semisimple. As $hV^t = V^t$, it follows that h is orthogonally decomposable on V . However, this is equivalent to saying that E has g -invariant non-abelian subgroups, against our assumption.

Suppose first that $\ell = 0$ or $(\ell, |S|) = 1$. Then we can apply [11, Theorem 9.18] (the case $r = 2$ being refined in [24, Lemma 4.4]). Thus $\rho_S^{\text{reg}} = M|_S + W$ if $\varepsilon = -1$ and $M|_S = \rho_S^{\text{reg}} + W$ if $\varepsilon = 1$, where W is a 1-dimensional FS -module. So in this case the lemma follows.

Next, suppose $(\ell, |S|) \neq 1$. We first show that the b -eigenspaces on M are all of dimension $|P|$, except one of dimension $|P| + \varepsilon$. Recall that M lifts to characteristic zero (this is true for every irreducible representation of a finite solvable group, e.g. see [39, p. 135]). As $(|B|, \ell) = 1$, the dimensions of the b -eigenspaces on M are the same as in the zero characteristic case. In the latter case the claim follows from (1) and (2)(i), already proven for characteristic zero.

Let $M = M_1 \oplus \cdots \oplus M_k \oplus M_0$, where M_1, \dots, M_k are the b -eigenspaces of dimension $|P|$ and M_0 is the b -eigenspace of dimension $|P| + \varepsilon$. Obviously, each of the M_i 's ($0 \leq i \leq k$) is P -stable.

Let L and $N = N_G(P)$ be as in Lemma 2.13. Observe that $N = N_E(P)S$. Moreover, as $[N_E(P), P] = E \cap P = 1$, we have $N_E(P) = C_E(P)$. We claim that $C_E(P) = Z(E)$. Indeed, by the argument above, every non-identity element of P acts fixed-point freely on the non-identity elements of $E/Z(E)$. It follows that $N = Z(E)S$ is abelian, and therefore, by Lemma 2.13, $L|_P$ is indecomposable. (Note that M is of non-zero defect as $\dim M$ is coprime to ℓ .) In particular, $\dim L < |P|$. Also notice that, since ρ_P^{reg} is indecomposable, the decomposition of $M|_P$ given in Lemma 2.13 consists of indecomposable summands. It follows, by the Krull-Schmidt theorem, that $M_i|_P \cong \rho_P^{\text{reg}}$ for $i = 1, \dots, k$, by dimension reasons. In addition, if $\varepsilon = -1$ then $M_0 \cong L$, whereas if $\varepsilon = 1$ then $M_0|_P = L \oplus \rho_P^{\text{reg}}$. We conclude that $M|_S$ is isomorphic to a submodule of of codimension 1 in ρ_S^{reg} , and $\dim L = |P| - 1$ if $\varepsilon = -1$, whereas if $\varepsilon = 1$ then $M|_S = \rho_S^{\text{reg}} \oplus L$ and $\dim L = 1$. So we get (1) and item (i) in (2).

Let U be as in (2)(ii). It follows from (2)(i) that the matrix of g on M is cyclic if and only if U does not contain L . The latter is equivalent to assertion (ii).

(iii) Obviously, the matrix of g is cyclic on every quotient module M/X provided X contains L . Let X be the kernel of the homomorphism $M \rightarrow (1 - z)M$. Then $L \subseteq X$ and $M/X \cong (1 - z)M$, as desired. (Note that $L \subset X$ because z is an ℓ -element, and therefore it acts as the identity on L .)

Corollary 3.3. *Let g, M be as in items (1) or (2) of Lemma 3.2. Then the matrix of g on M is almost cyclic.*

Corollary 3.4. *Let g, M be as in items (1) or (2) of Lemma 3.2, and let $h \in \langle g \rangle$ be such that $1 \neq |h| < |g|$. Then the matrix of h on M is not almost cyclic, except for the case where $r^n = 3$, $|g| = 4$ and $|h| = 2$.*

Proof. Set $T = \langle h \rangle$ and let $d = |S : T| = |g|/|h|$. In case (2) of Lemma 3.2 we have that $M|_T = d \cdot \rho_T^{\text{reg}} \oplus L|_T$, so the claim is obvious. In case (1) $M|_T$ is of codimension 1 in $d \cdot \rho_T^{\text{reg}}$ so we are done unless $d = 2$ and $|T| = 2$. However, if $2 = |T| = |g|/2 = (r^n + 1)/2$ then $3 = r^n$, whence $r = 3$ and $n = 1$. If $r = 3$ and $n = 1$, then $|g| = 4$ and $|h| = 2$. In this case h is obviously almost cyclic.

Corollary 3.5. *Let $G = E\langle g \rangle \subset GL(r^n, F)$, where E is a normal subgroup of symplectic type, $|E/Z(E)| = r^{2n}$, $C_{\langle g \rangle}(E) = 1$, $C_E(g) = Z(E)$ and g is of order coprime to r . Let \bar{g} be the projection of g into $Sp(2n, r) \subset \text{Aut } E$. Suppose that \bar{g} is orthogonally indecomposable and g is almost cyclic. Then \bar{g} is of order $r^n + 1$ or $r^n - 1$.*

Proof. Set $V = E/Z(E)$. Then V is a non-degenerate symplectic space and \bar{g} is completely reducible as an element of $Sp(2n, r)$. Moreover, it is well known that either \bar{g} is irreducible or it preserves a totally isotropic subspace of V . In fact, in the second case the assumptions that $(|g|, r) = 1$ and \bar{g} is orthogonally indecomposable, imply that \bar{g} preserves a maximal totally isotropic subspace of V . Now, suppose we are in the former case. Then $|\bar{g}|$ divides $r^n + 1$. Let g_1 be an element of order $r^n + 1$ in $Sp(2n, r)$ such that $\bar{g} \in \langle g_1 \rangle$. Then, by Corollaries 3.3 and 3.4, $|g_1| = |\bar{g}|$, and we are done.

In the latter case \bar{g} has order dividing $r^n - 1$, and the result again follows with same argument, as in the former case, from Corollaries 3.3 and 3.4.

Corollary 3.6. *Let g, M be as in items (1) or (2) of Lemma 3.2. In addition, suppose that $|g| = p^a$ for some integer $a > 0$ and some prime p . Then one of the following holds:*

- (1) $r = 2$, and either $|g| = p$ is a Fermat or Mersenne prime, or $|g| = 9$;
- (2) r is odd, and either $n = 1$, $|g| = 2^a$ for some integer a and r is a Fermat or Mersenne prime, or $r^n = 9$ and $|g| = 8$.

Proof. As $|g| = p^a = r^n + 1$ or $r^n - 1$, it follows from Lemma 2.6 that either p or r equals 2. Moreover, if $p^a = r^n + 1$ then either $p = 2, n = 1$ or $r = 2, a = 1$ or $p^a = 9$. If $p^a = r^n - 1$, then $p^a + 1 = r^n$. So again either $r = 2, a = 1$ or $p = 2, n = 1$ or $r^n = 9$. Thus, if r is odd, then either $r^n = 9$ or $p = 2$ and r is a Fermat or Mersenne prime; if $r = 2$ then either $|g| = 9$ or $|g|$ is a Fermat or Mersenne prime.

Lemma 3.7. *Let $G = E\langle g \rangle$, where E is a normal subgroup of G of symplectic type, $|E/Z(E)| = r^{2n}$ and $|g|$ is a prime-power coprime to r . Let \bar{g} be the projection of g into $Sp(2n, r)$. Let $\phi \in \text{Irr}_F G$ be faithful with $r \neq \ell$. Suppose that $\phi(g)$ is almost cyclic. Then \bar{g} is orthogonally indecomposable in $Sp(2n, r)$ and $|\bar{g}| = r^n + 1$ or $r^n - 1$. Moreover, $|\text{Spec } \phi(g)| = r^n$ in the former case and $r^n - 1$ in the latter case.*

Proof. Set $V = E/Z(E)$. Then we may write $V = V_1 \oplus \cdots \oplus V_k$, where the V_i 's, for $i = 1, \dots, k$, are non-degenerate, mutually orthogonal, orthogonally indecomposable subspaces of V invariant under the action of \bar{g} . Thus $\bar{g} = \text{diag}(h_1, \dots, h_k)$, where $h_i = \bar{g}|_{V_i}$ for $i = 1, \dots, k$. Let H_i denote the group $Sp(V_i)$, for $i = 1, \dots, k$, so that $h_i \in H_i$. Set $H = H_1 \times \cdots \times H_k$. By Lemma 3.1, $\phi|_E$ is irreducible, and hence ϕ has degree r^n . It is also well known (e.g. see [16]) that $\phi|_E$ extends to a representation τ , say, of the semidirect product EH such that the restriction $\tau|_H$ is the tensor product of the generic Weil representations τ_i of the groups H_i , having degree r^{n_i} , where $n_i = \dim V_i/2$, and moreover $\tau(\bar{g})$ differs from $\phi(g)$ by a scalar multiple. In particular, $\tau(\bar{g})$ is also almost cyclic. As $\tau(\bar{g}) = \tau_1(h_1) \otimes \cdots \otimes \tau_k(h_k)$, it follows that $\tau_i(h_i)$ is almost cyclic for every i . Now, suppose that $h_i = \bar{g}|_{V_i} \neq \text{Id}_{V_i}$. As h_i satisfies the assumptions of Corollary 3.5, it follows that h_i has order $r^{n_i} + 1$ or $r^{n_i} - 1$. As $|g|$ is a prime-power, using properties of Zsigmondy primes we readily deduce that $|h_i| = |h_j|$, unless $|h_i| = 1$ or $|h_j| = 1$ ($1 \leq i, j \leq n$). As $\tau(\bar{g})$ is almost cyclic, it follows that $|h_i| \neq 1$ only for one of the i 's. We can assume that this i is 1. Assume that $k > 1$. Then $\tau(\bar{g}) = \tau_1(h_1) \otimes \text{Id}_m$, where $m > 1$. But then $\tau(\bar{g})$ is not almost cyclic, and hence also $\phi(g)$ is not almost cyclic, against our assumptions. Thus $k = 1$, and Corollary 3.5 applies. The additional claim on $\text{Spec } \phi(g)$ follows from Lemma 3.2.

Lemma 3.8. *Let $H = \langle g \rangle$ be a cyclic r -group (r a prime) and let $\phi : H \rightarrow GL(n, F)$ be a complex representation of H with character χ . Suppose that $\chi(g^i) = 0$ for $(i, |g|) = 1$ and λ be an eigenvalue of g^r of multiplicity d . Then all the μ 's in F such that $\mu^r = \lambda$ are eigenvalues of g of multiplicity d/r .*

Proof. See [10, Lemma 2.4].

We recall here that an irreducible subgroup of $GL(V)$, where V is a vector space over a field F , is said to be primitive on V if it does not preserve any direct sum decomposition of V into non-trivial subspaces of equal dimension.

The following lemma essentially follows from Clifford theory.

Lemma 3.9. *Let G be a finite primitive subgroup of $GL(V)$, where V is a finite-dimensional vector space over F . Let $S(G)$ denote the maximal solvable normal subgroup of G . Suppose that $S(G) \neq Z(G)$. Then the following holds:*

- (1) G contains a normal r -subgroup E of symplectic type for some prime r (so, the group E has exponent r if r is odd, whereas it has exponent 4 if $r = 2$). Furthermore, $r \neq \ell$.

(2) If G is tensor-indecomposable, then E is irreducible and $\dim V = r^n$, where $|E/Z(E)| = r^{2n}$.

Proof. (1) Let E be a minimal non-central solvable normal subgroup of G . Then, by Clifford's theorem, E is non-abelian. Furthermore, $Z(E)$ consists of scalar matrices and the commutator subgroup E' is contained in $Z(E)$. So $E/Z(E)$ is abelian. As E is nilpotent, again the minimality assumption implies that E is a r -group for some prime r , and hence is an r -group with no non-cyclic characteristic subgroups. Moreover $O_\ell(G) = 1$, as G is irreducible, whence $r \neq \ell$. Next, suppose that r is odd. Then one easily sees that E contains a non-central element of order r . Let $\Omega_1(E)$ denote the subgroup of E generated by all its elements of order r . Then $\Omega_1(E) = E$. As $E/Z(E)$ is abelian, any two elements of E commute mod $Z(E)$. It follows that $E/Z(E)$ has exponent r , which in turn implies that $|E'| = r$. Indeed, let $x, y \in E$. As $y^r \in Z(E)$, $1 = [y^r, x] = [x, y]^r$. As E' is cyclic, $|E'| = r$. Now, for any $x, y \in E$, $(xy)^r = x^r y^r [x, y]^{r(r-1/2)} = x^r y^r$. Thus, if x and y have order r , xy also has order r . As $\Omega_1(E) = E$, we deduce that E has exponent r . Finally, suppose that $r = 2$. If E does not contain non-central involutions, then E is the quaternion group of order 8. Otherwise, arguing as above one sees that $E/Z(E)$ has exponent 2 and E has exponent 4.

(2) It follows from Clifford theory (e.g. see [53, pp. 139 - 141]) that if G is a primitive subgroup of $GL(n, R)$, where R is an algebraically closed field, then G can be viewed as a subgroup of the tensor product $G_1 \otimes \cdots \otimes G_m$, where G_i for $1 \leq i \leq m$ is a primitive tensor-indecomposable subgroup of $GL(n_i, R)$, $n = n_1 \cdots n_m$, and every normal subgroup of G_i is either irreducible or scalar. As G in (2) is assumed to be tensor-indecomposable, we have that $m = 1$, and the result follows from (1).

Theorem 3.10. *Let G be a primitive subgroup of $GL(m, F)$ with non-central maximal solvable normal subgroup $S(G)$. Suppose that $G = \langle g^G \rangle$, where g is almost cyclic and $g^p \in Z(G)$ for some prime $p > 2$. Then G contains an irreducible normal r -subgroup E of symplectic type, and one of the following holds:*

(1) $m = p = r$ and $G = Z(G) \cdot E \cdot Sp(2, r)$.

(2) $m = 2^n$ for some natural number n , $|E/Z(E)| = 2^{2n+1}$ and $\overline{G} := G/(Z(G)E)$ is isomorphic to a subgroup of $Sp(2n, 2)$ generated by a conjugacy class of elements \overline{g} of order $p = 2^n - 1$ or $2^n + 1$.

Proof. As, by assumption, the p' -part of g is scalar, we may assume that $|g|$ is a p -power without loss of generality. By Lemma 3.9, G contains a normal r -subgroup E of symplectic type for some prime r , where $r \neq \ell$ and $Z(E) \subseteq Z(G)$. Let $|E/Z(E)| = r^{2n}$. Set $K := \langle E, g \rangle$. As $G = \langle g^G \rangle$ and $C_G(E)$ is normal in G , we have $[E, g] \neq 1$. Let V be the underlying space of $GL(m, F)$. We shall show that E acts on V irreducibly.

Assume first that $(|g|, \ell) = 1$, where $\ell = \text{char} F$. Then V is completely reducible as an FK -module. Let $V = V_1 \oplus \cdots \oplus V_t$, where the V_i 's are irreducible FK -submodules. Therefore, every V_i is a faithful irreducible FE -module (see Lemma 3.1). So $\dim V_i = r^n$ for every $i = 1, \dots, t$. For each i let g_i be the projection of g to V_i . Then g_i is almost cyclic. Let μ be an eigenvalue of g . Then the μ -eigenspace of g is the sum of the μ -eigenspaces of some of the g_i 's.

We have two cases: (a) $(|g|, r) = 1$; (b) $|g|$ is an r -power.

In case (a), let $g^p = \lambda \cdot \text{Id}$, where $\lambda \in F$. By Lemma 3.7, g_i^d is scalar in $GL(V_i)$ where $d = r^n \pm 1 = p$, so $g_i^d = \lambda \cdot \text{Id}$. Moreover, all the p -roots of λ , except one of them when $d = p = r^n + 1$, occur as eigenvalues of g_i . Therefore, at least two eigenvalues ν, μ of g are common on V_1 and $V_2 \oplus \cdots \oplus V_t$. This contradicts the assumption that g is almost cyclic, unless $t = 1$, that is V is irreducible as an FE -module, or $p = 3$, $t = 2$. In the latter case, we have $r = 2$, $n \leq 2$.

In case (b), where $r = p$, by [10, Lemma 2.5], either $|E| = p^3$ or $p = 3$ and $|E| = 3^5$. In the latter case $n = 2$ and, again by [10, Lemma 2.5], g has $r^n = 3^2$ distinct eigenvalues

which is false as g^3 is scalar. In the former case, by [10, Lemma 2.5], g is cyclic and hence $m \leq p = r$ unless, possibly, when $p = 3$, which implies $t = 2$. So either $t = 1$, or $t = 2$ and $p = 3$.

Next, suppose that g is an ℓ -element, that is $p = \ell \neq r$, and hence $g^p = 1$. Let $V_1 \subset V_2 \subset \cdots \subset V_t = V$ be a composition series for $K = \langle E, g \rangle$. Then every composition factor is a faithful irreducible FE -module. Denote by $g|_{V_2/V_1}$ the element of $GL(V_2/V_1)$ induced by g on V_2/V_1 . Then, by Lemma 3.7, $p = |g| = r^n \pm 1$, and so by Lemma 3.2 the Jordan forms of $g|_{V_1}$ and $g|_{V_2/V_1}$ contain a block of size at least $|g| - 1$. As g is almost cyclic, again we must have either $t = 1$, or $p = 3$ and $V = V_2$. In the latter case we get $r = 2$ and $n \leq 2$.

Now, let $t = 2$, $p = 3$. Observe that G is tensor-decomposable for $t > 1$ (see Lemma 3.9(2)). As $t = 2$, we have $zg = g_1 \otimes g_2$ for some scalar matrix z where $g_1 \in GL(m/2, F)$ and $g_2 \in GL(2, F)$. By Lemma 2.2, both g_1 and g_2 are cyclic. Recall that $\text{Id} \otimes g_2$ centralizes E and $g_1 \otimes \text{Id}$ normalizes E and produces the same automorphism on E as g . Therefore, g_1^3 and g_2^3 are scalar. Therefore $\dim V_1 \leq 3$. Suppose first that $\ell \neq 3$. Assume $\dim V_1 = 3$. Then both g_1 and g_2 have trace zero. It follows that the traces of $zg = g_1 \otimes g_2$ and $z^2g = g_1^2 \otimes g_2^2$ are 0. Hence the traces of g and g^2 are also zero. By Lemma 3.8, g is not almost cyclic. Therefore, $\dim V_1 = 2$ and hence $r = 2$. So $G/Z(G)E \subseteq SL(2, 2)$, and hence $G/Z(G)E$ is of order 3 (as $G/Z(G)E$ is generated by the conjugates of \bar{g}). We conclude that $G = K$, and the claim that E is irreducible follows, again by Lemma 3.1.

Next, let $\ell = 3$. Then $|g_1| = |g_2| = 3$. If $\dim V_1 = 2$, then $r = 2$ and we have $G = K$ and $t = 1$, as above. Let $\dim V_1 = 3$. As g_1 is cyclic, the Jordan form of g_1 is a single block, and hence the Jordan form of $g_1 \otimes g_2$ consists of 2 blocks of size 3, which is false as zg is almost cyclic.

Thus, in view of the above, $V = V_1$, which means that $m = r^n$. Suppose $r = p$. Then, as already seen above, $|E| = p^3$ and $n = 1$, which implies (1). Next, let $(r, p) = 1$. Let N be the normalizer of E in $GL(m, F)$. Then $N/EZ(N) \cong Sp(2n, r)$. Let \bar{g} be the projection of g into $Sp(2n, r)$. By Lemma 3.7, $|\bar{g}| = r^n \pm 1$. So $r = 2$ and we have (2).

4. SOME LOW-DIMENSIONAL CLASSICAL GROUPS

In this Section, we first consider semisimple elements of prime-power order of a group G such that $SL(2, q) \subseteq G \subseteq GL(2, q)$, and determine the irreducible F -representations of G in which such elements are represented by almost cyclic matrices. Next, we obtain results of the same kind for some other small dimensional linear groups (see Lemmas 4.11, 4.13, 4.14), which will be needed in Section 5 in order to deal with the general case when $SL(n, q) \subseteq G \subseteq GL(n, q)$, for any $n > 2$. Finally, in Lemmas 4.15, 4.16, 4.17 and 4.18 we examine some low-dimensional symplectic and unitary groups which will also play a role in Section 5. We emphasize that in this Section, we do not restrict ourselves to Weil representations.

Lemma 4.1. *Let $SL(2, q) \subseteq G \subseteq GL(2, q)$. Then every irreducible F -representation of G lifts to characteristic zero.*

Proof. Denote by Z the set of non-zero scalar matrices in $GL(2, q)$. Let τ be an irreducible F -representation of G . Obviously, τ extends to $Z \cdot G$, and τ lifts if and only if the extension lifts. Note that $Z \cdot G$ is of index at most 2 in $GL(2, q)$, so either $Z \cdot G = GL(2, q)$ or $Z \cdot G = Z \cdot SL(2, q)$.

The shapes of the decomposition matrices modulo ℓ for $SL(2, q)$ show that the lemma is true for this case, see for instance [3, Ch. 9]. (The reader should note that this does not hold for $PSL(2, q)$, e.g. see [4].) Therefore, it suffices to prove the lemma for $G = GL(2, q)$, q odd.

Assuming this, set $X = Z \cdot SL(2, q)$ and $\tau_1 = \tau|_X$. Suppose first that τ_1 is irreducible. Let ϕ_1 be the lift of τ_1 . Looking at the character tables of $SL(2, q)$ and $GL(2, q)$, one observes that τ_1 extends to G . Let ϕ be the extension, and set $\tau_2 = \phi \pmod{\ell}$. A priori,

τ_2 may not coincide with τ . However, for every $g \in G$ the conjugation by $\tau(g)$ and $\tau_2(g)$ yields the same automorphism of $\tau(X)$. By Schur's lemma, $\tau_2(g) = \tau(g)\lambda(g)$ for some $\lambda(g) \in F$. One readily checks that $g \rightarrow \lambda(g)$ is a group homomorphism. Therefore, $\tau_2 = \tau \otimes \lambda$. As λ is one-dimensional, λ lifts to characteristic zero. Let μ be the lift of λ . Then $(\mu^{-1} \otimes \phi) \pmod{\ell} = \tau$, as required.

Next, suppose that τ_1 is reducible, and hence completely reducible by Clifford's theorem. Then τ_1 has two irreducible constituents σ_1, σ_2 , say, which are G -conjugate, and hence are of equal dimension, which is at most $(q+1)/2$. As G/X is cyclic, it follows from Clifford's theory that σ_1, σ_2 are not equivalent (see for instance [26, Th. 19.13]). Let ϕ_1, ϕ_2 be lifts of σ_1, σ_2 , respectively. Then ϕ_1, ϕ_2 are not equivalent, and have equal dimension at most $(q+1)/2$. Moreover, $\phi_1|_Z = \phi_2|_Z$; therefore, $\phi_1|_{SL(2,q)} = \phi_2|_{SL(2,q)}$ are not equivalent. It is well known that $SL(2, q)$ has exactly two non-equivalent complex representations of equal degree (which is either $(q+1)/2$ or $(q-1)/2$), and they are G -conjugate. It follows from the character table of $G = GL(2, q)$ that there exists an irreducible representation ψ of G such that $\psi|_X = \phi_1 \oplus \phi_2$. Set $\tau'_2 := \psi \pmod{\ell}$. Then τ'_2 is irreducible (as neither σ_1 nor σ_2 is G -stable). Then we claim that τ'_2 is equivalent to τ . Obviously, the Brauer character of $\tau'_2|_X$ coincides with that of $\tau|_X$. Let $g \in G$, $g \notin X$. Then g permutes σ_1, σ_2 , and hence the matrix of $\tau'_2(g)$ has zero trace. More precisely, both the Brauer character values of $\tau'_2(g)$ and $\tau(g)$ are 0 (see, for instance, [8, Proposition 2.14]). It follows that the Brauer characters of τ'_2 and τ coincide, and hence τ'_2 and τ are equivalent.

Lemma 4.2. *Let $SL(2, q) \subseteq G \subseteq GL(2, q)$, $q > 3$, $Z = Z(GL(2, q))$, and let T be the subgroup consisting of the diagonal matrices in G . Let τ an irreducible F -representation of G , such that $\tau|_{Z(G)} = \zeta \cdot \text{Id}$, where $\zeta \in \text{Irr } Z(G)$.*

(1) *Suppose that q is odd and $\dim \tau = (q-1)/2$. Then $G \subseteq Z \cdot SL(2, q)$ and*

$$\tau|_T = \zeta^T.$$

(2) *Suppose that q is odd and $\dim \tau = (q+1)/2$. Then $G \subseteq Z \cdot SL(2, q)$ and*

$$\tau|_T = \nu \oplus \zeta^T,$$

where ν is a 1-dimensional representation of T .

(3) *Suppose that $\dim \tau = q-1$. Then*

$$\tau|_T = \zeta^T,$$

unless $G \subseteq Z \cdot SL(2, q)$, in which case $\tau|_T = 2 \cdot \zeta^T$.

(4) *Suppose that $\dim \tau = q+1$. If $G \subseteq Z \cdot SL(2, q)$ and q is odd, then*

$$\tau|_T = \mu \oplus 2 \cdot \zeta^T,$$

where μ is a 2-dimensional representation of T .

If q is even or $G \not\subseteq Z \cdot SL(2, q)$, then

$$\tau|_T = \mu \oplus \zeta^T,$$

where μ is a 2-dimensional representation of T .

(5) *Suppose that $\dim \tau = q$. Then $\tau|_T = \nu \oplus c \cdot \zeta^T$, where ν is a 1-dimensional representation of T , and $c = 1$ if q is even or $G \not\subseteq Z \cdot SL(2, q)$, otherwise $c = 2$.*

Proof. By Lemma 4.1, τ lifts to characteristic zero. Let χ be the character of the lift.

Let U be the abelian subgroup of order q consisting of the upper unitriangular matrices in G . Then T normalizes U and $C_T(u) = Z(G)$ for every $1 \neq u \in U$. Set $K = \text{Irr } U$. Acting on U by conjugation, T has a single orbit on $U \setminus \{1\}$ if q is even or $G \not\subseteq Z \cdot SL(2, q)$, and two orbits of size $(q-1)/2$ if q is odd and $G \subseteq Z \cdot SL(2, q)$. Then this is also true for the (dual) action of T on K .

Let M be the module afforded by τ . For $\alpha \in K$, set $M_\alpha = \{m \in M : \tau(u)m = \alpha(u)m \text{ for all } u \in U\}$. Then T permutes the (non-zero) M_α 's. It follows that, for every T -orbit

O on the M_α 's, T stabilizes the subspace $M_O := \sum_{\alpha \in O} M_\alpha$. Note that $Z(G) \subseteq T$. It is easy to observe that the restriction of $\tau|_T$ to M_O yields a representation of T equivalent to ζ^T , where $\zeta \in \text{Irr } Z(G)$, $xm = \zeta(x)m$ for $x \in Z(G)$ and $m \in M_O$. As M is irreducible, it is clear that ζ is the same for every T -orbit O .

Suppose first that $\tau(1) = (q \pm 1)/2$. Then $G \subseteq Z \cdot SL(2, q)$. By the above, applying Clifford's theorem to TU , it follows that, if $\dim \tau = (q - 1)/2$, then $\tau|_U$ is the sum of the characters of a T -orbit of length $(q - 1)/2$, whereas, if $\dim \tau = (q + 1)/2$, then $\tau|_U$ is the sum of 1_U (with multiplicity 2) and the characters belonging to a T -orbit of size $(q - 1)/2$.

Next, suppose that $\chi(1) \in \{q - 1, q, q + 1\}$. Then $\tau|_U = \rho_U^{reg} + a \cdot 1_U$, where $a = \chi(1) - q$. Therefore, for any τ , the restriction $\tau|_U$ is the sum of one-dimensional representations of U , each of multiplicity one, except when $\chi(1) = q + 1$, in which case 1_U has multiplicity 2 and the other irreducible constituents have multiplicity 1.

This immediately implies all the statements of the lemma.

Lemma 4.3. *Let $SL(2, q) \subseteq G \subseteq GL(2, q)$, and let $1 \neq g \in G$ be a semisimple element of p -power order, where p is an odd prime. Let M be an irreducible FG -module with $\dim M > 1$ and let τ be the representation afforded by M . Then $\tau(g)$ is almost cyclic if and only if $\dim M \leq |g| + 1$. Moreover, in this case $(2, q + 1) \cdot |g|$ equals $q + 1$ or $q - 1$.*

Proof. Firstly note that, by our assumptions, $q > 3$. Let P be a Sylow p -subgroup of G . As $Z \cdot SL(2, q)$ has index at most 2 in G , we have $P \subset Z \cdot SL(2, q)$. It follows that it suffices to prove the result for $G = SL(2, q)$. Indeed, this is trivial if $G \subseteq Z \cdot SL(2, q)$. So, assume otherwise. Then $Z \cdot G = GL(2, q)$, and hence we may assume $G = GL(2, q)$. The claim is obvious if $\tau(SL(2, q))$ is irreducible. If not, by Clifford's theorem, $\tau(SL(2, q))$ is a direct sum of two irreducible constituents, permuted by any element of $x \in G$, which is not in $Z \cdot SL(2, q)$. Note that an element $x \in GL(2, q)$ belongs to $Z \cdot SL(2, q)$ if and only if $\det x$ is a non-zero square in F_q , and hence there is $x \in C_{GL(2, q)}(P)$, which is not in $Z \cdot SL(2, q)$. Therefore, y permutes the irreducible constituents of $\tau|_{SL(2, q)}$ and commutes with P . This implies that both of them have the same restriction to P , and hence no non-scalar element of $\tau|_P$ is almost cyclic.

Thus, we may assume that $G = SL(2, q)$. By Lemma 4.1, τ lifts to characteristic zero. So, if $p \neq \ell$, it suffices to verify the lemma for $\ell = 0$, which can be easily done examining the character table of G . Therefore, from now on we assume $p = \ell$.

In this case P is cyclic, and we assume that $g \in P$. As p is odd and $\dim M \in \{(q \pm 1)/2, q \pm 1, q\}$, it follows that p divides $\dim M$ if and only if so does $|P|$. It is also well known (e.g. see [3]) that every FG -module is either of defect 0 or of defect d , where $|P| = p^d$.

If g is diagonalizable (equivalently, $|g|$ divides $q - 1$), then the statement of the lemma about the almost cyclicity of $\tau(g)$ follows from Lemma 4.2, except, possibly, for the case where q is even, $\dim M = q + 1$, $|P| = |g| = q - 1$ and $\mu(g)$ in Lemma 4.2(4) is scalar. However, as $N_G(P)/P$ is cyclic, this contradicts the almost cyclicity of $\tau(g)$ by Corollary 2.14.

Therefore, we may assume that g is not diagonalizable (and hence $|g|$ divides $q + 1$).

If $|P|$ divides $\dim M$, then $M|_P$ is a projective FP -module, and hence $M|_P = m \cdot \rho_P^{reg}$ for some integer $m > 0$. Then, obviously, the matrix of $\tau(g)$ is almost cyclic if and only if $m = 1$ and $|g| = |P| = \dim M$, in which case $\tau(g)$ is cyclic.

Thus, from now on we assume that $|g|$ is coprime to $\dim M$.

By Lemma 2.13 and Corollary 2.14, we have two options: either

- (i) $\dim M < |P|$ and $M|_P$ is indecomposable; or
- (ii) $M|_P = \rho_P^{reg} \oplus L|_P$, where $L \neq 0$ is an irreducible $FN_G(P)$ -module trivial on P .

Suppose that (i) holds, and let $g = h^{p^b}$, where $P = \langle h \rangle$ and $b \geq 0$. Then the matrix of $\tau(h)$ is a Jordan block of size $t = \dim M$. So we are done if $b = 0$, that is, $|g| = |P|$. Suppose that $b > 0$, that is, $|g| < |h|$. By [9, Lemma 5.4], the Jordan form of g on M contains at least two non-trivial blocks of equal size (and hence the matrix of $\tau(g)$ is not almost cyclic) unless

$t = p^{d-1} + 1$ and $\tau(g)$ is a transvection. In the latter case $\tau(G)$ is an irreducible subgroup of $GL(M)$ generated by transvections. The finite irreducible subgroups of $GL(M)$ generated by transvections are well known (see [49], [58]). Since $\ell = p \neq 2$, these are isomorphic to $SL(t, F_{\ell^m})$, $SU(t, F_{\ell^m})$, $Sp(t, F_{\ell^m})$, or $SL(2, 5) \subset SL(2, F)$ for $\ell = 3$. Clearly, none of these groups are isomorphic to $\tau(G)$. (Note that, as $(\ell, q) = 1$ and $\ell \neq 2$, the isomorphisms $\tau(SL(2, 7)) \cong SL(3, 2)$ and $\tau(SL(2, 5)) \cong SL(2, 4)$ should be ignored.)

Now, suppose that (ii) holds (that is, $M|_P = \rho_P^{reg} \oplus L|_P$). Clearly, $|g| = |P|$, as the matrix of $\tau(g)$ is almost cyclic. Furthermore, since $N_G(P)$ has an abelian normal subgroup of index 2, by Clifford's theorem $0 < \dim L \leq 2$. Whence $|P| < \dim M \leq |P| + 2$.

Suppose first that q is even. As $|P| < \dim M$, we have $|P| < q + 1$, and hence $|P| \leq (q+1)/3$. Therefore, as $\dim M \geq q-1$, $q-1 \leq |P|+2 \leq (q+7)/3$, and hence $3q-3 \leq q+7$, that is $q = 4$. However, this forces $|P| = 5 = q + 1$, which is not the case.

So, suppose that q is odd. Then $|P| \leq (q+1)/2$, which implies $\dim M \leq \frac{q+1}{2} + 2$.

If $|P| = (q+1)/2$, then $\dim M > |P| = (q+1)/2$ implies $\dim M = q-1, q$ or $q+1$, but the latter option is ruled out, as $|P|$ is coprime to $\dim M$. So $q-1 \leq 2 + \frac{q+1}{2}$, whence $q \leq 7$. However, $q \neq 7$, as $p > 2$. So $q = 5$, whence $|g| = |P| = 3$ and $\dim M = 4, 5$. Suppose that $\dim M = 5$. Then M is a $PSL(2, 5)$ -module, and in $PSL(2, 5)$ the quotient $N(P)/P$ is abelian. This forces $\dim L = 1$, whence $\dim M = 4$, as $M|_P = \rho_P^{reg} \oplus L$. A contradiction. So $\dim M = 4$, and we are done.

If $|P| < (q+1)/2$, then $|P| \leq (q+1)/4$, and hence $(q-1)/2 \leq \dim M \leq 2 + (q+1)/4$, whence $q \leq 11$. The case $q = 5$ is ruled out, as $|g| < (q+1)/2$ implies $|g| < 3$. As above, the case $q = 7$ is also ruled out, as $p > 2$. Finally, in both the cases $q = 9, 11$, M is a $PSL(2, q)$ -module, and in $PSL(2, q)$ the quotient $N(P)/P$ is abelian, whence $\dim L = 1$. A contradiction, as $M|_P = \rho_P^{reg} \oplus L$ would then imply $\dim M = 6$ for $q = 9$ and $\dim M = 4$ for $q = 11$, which is impossible.

As for the last claim in the statement, note that $|g|$ divides $q + \varepsilon$, where $\varepsilon = 1$ or -1 . Let q be odd. If $|g| = (q + \varepsilon)/2$, then the claim is true, otherwise $|g| \leq (q + \varepsilon)/4$. As $\dim M \geq (q-1)/2$, we have $(q-1)/2 \leq \dim M \leq 1 + \frac{q+\varepsilon}{4}$, whence $q \leq 6 + \varepsilon$. But then $|g| \leq 2$, a contradiction. Now, suppose that q is even. Then $q + \varepsilon$ is odd, and hence either $|g| = q + \varepsilon$, as required, or $|g| \leq (q + \varepsilon)/3$. As $\dim M \geq q-1$, we have $q-1 \leq \dim M \leq 1 + \frac{q+\varepsilon}{3}$, whence $2q < 6 + \varepsilon$, a contradiction, as $q > 3$.

At this stage, we are left to deal with the case where $SL(2, q) \subseteq G \subseteq GL(2, q)$, and $1 \neq g \in G$ is a semisimple element of 2-power order.

We begin with an auxiliary Lemma:

Lemma 4.4. *Let $SL(2, q) \subseteq G \subseteq GL(2, q)$, where $q > 3$ is odd, and let g be a non-scalar 2-element of G . Let $\ell = 2$, and let M be an irreducible FG -module of dimension $m > 1$, affording the representation τ . Suppose that $\tau(g)$ is a transvection. Then one of the following holds:*

- (1) $G = SL(2, 5)$, $m = 2$ and $\tau(G) = SL(2, 4)$;
- (2) $G = SL(2, 7)$, $m = 3$ and $\tau(G) = SL(3, 2)$;
- (3) $G = GL(2, 5)$, $m = 4$ and $\tau(G) = O^-(4, 2)$.

Proof. Let G_1 be the subgroup of G generated by the G -conjugates of g . Clearly, G_1 is a (normal) subgroup of G containing $SL(2, q)$. It follows that $\tau(G)$ is irreducible. Indeed, otherwise, by Clifford's theorem $M|_{G_1} = M_1 \oplus M_2$, where M_1, M_2 are G -conjugate irreducible constituents (this is because $M|_{SL(2, q)}$ is either irreducible or the sum of two irreducible constituents). Hence, every element of G_1 non-trivial on M_1 is also non-trivial on M_2 . However, a transvection stabilising M_1 and M_2 must be trivial either on M_1 or on M_2 . This is a contradiction.

Thus, M is an irreducible FG_1 -module. Set $G_2 = \tau(G_1)$. By Lemma 2.12, either m is even and $G_2 \in \{S_{m+1}, S_{m+2}, SL(m, q_1), Sp(m, q_1), O^\pm(m, q_1), SU(m, q_1)\}$, or m is odd and $G_2 \in \{SL(m, q_1), SU(m, q_1)\}$, where q_1 is even in all the cases. It follows that one of the following holds: (i) $G_1 = SL(2, 5)$ and $G_2 = SL(2, 4)$, $m = 2$; (ii) $G_1 = SL(2, 7)$ and

$G_2 = SL(3, 2)$, $m = 3$; (iii) $G_1 = GL(2, 5)$ and $G_2 = O^-(4, 2)$, $m = 4$. (Note that the group $Sp(4, 2)$ is not isomorphic to $PGL(2, 9)$ (e.g., see [5, p. 4]), so the case $G = GL(2, 9)$ does not occur in our list.)

In the cases (i) and (ii) $|G : G_1| \leq 2$, so either $G = G_1$ or $G = GL(2, 5)$ and $GL(2, 7)$, respectively. The latter options are ruled out, as neither $GL(2, 5)$ nor $GL(2, 7)$ have 2-modular irreducible representations of degree 2 or 3. In case (iii), we have $G = G_1$. This completes the proof.

Remark. In order to simplify the proof of some of the subsequent lemmas, it is worth observing explicitly at this point that, if one wishes to examine the representations of a group G , where $SL(2, q) \subseteq G \subseteq GL(2, q)$, it is enough to consider the cases $G = GL(2, q)$ and $G = SL(2, q)$. Indeed, let M be an irreducible FG -module. Set $Z = Z(GL(2, q))$, and $G_1 = G \cdot Z$. Obviously, M extends to an FG_1 -module. Now, G_1 contains $SL(2, q) \cdot Z$. As the latter subgroup has index at most 2 in $GL(2, q)$, it follows that, without loss of generality, we may assume either $G = SL(2, q)$ or $G = GL(2, q)$.

Furthermore, note that, for $\ell = 2$ it is sufficient to deal with the groups $PSL(2, q)$ and $PGL(2, q)$. This is obvious if $G = SL(2, q)$. If $G = GL(2, q)$, let Z_2 denote the Sylow 2-subgroup of $Z(G)$. Then Z_2 is in the kernel of M , so M can be viewed as an $F(G/Z_2)$ -module. Set $\bar{G} = G/Z_2$ and observe that $\bar{G} = Z(\bar{G}) \times K$, where $K \cong PGL(2, q)$. Whence the claim. See also the proof of Lemma 2.2 in [47].

Lemma 4.5. *Let $SL(2, q) \subseteq G \subseteq GL(2, q)$, where $q \equiv 1 \pmod{4}$, let $g \in G \setminus Z(G)$ be a 2-element, and let h be the projection of g into $G/Z(G)$. Let M be an irreducible FG -module of dimension $m > 1$, and let τ be the representation afforded by M . Then $\tau(g)$ is almost cyclic if and only if the following holds:*

- (1) $\ell \neq 2$, $g \in SL(2, q) \cdot Z(GL(2, q))$, $\dim M = (q \pm 1)/2$ and $|h| = (q - 1)/2$;
- (2) $\ell \neq 2$, $g \notin SL(2, q) \cdot Z(GL(2, q))$, and either $\dim M = q$ or $q - 1$ and $|h| = q - 1$, or $q = 5$, $\dim M = 4$, $|g| = 8$ and $|h| = 2$;
- (3) $\ell = 2$ and either $\dim M \leq |h| + 1$ or $G = GL(2, 5)$, $\tau(G) \cong O^-(4, 2)$, $m = 4$ and $\tau(g)$ is a transvection.

Proof. Note that, by the remark above, we may assume either $G = SL(2, q)$ or $G = GL(2, q)$.

Let us suppose that $\ell = 0$. Assume first that $|g|$ does not divide $q - 1$. In this case $G \neq SL(2, q)$ (otherwise $|g|$ divides $q + 1$, but $(q + 1)/2$ is odd, so $|g| = 2$, and hence g would be scalar). So, let $G = GL(2, q)$. Then g is irreducible and g^2 is scalar (as $(q^2 - 1)/(q - 1) = q + 1$ and $(q + 1)/2$ is odd). Thus $\tau(g)$ has exactly two distinct eigenvalues. As $\tau(g)$ is almost cyclic, $\tau(g)$ is a pseudo-reflection. It then follows from ([20, Lemma 3.1]) that G can be generated by at most 4 conjugates of g , whence, by Lemma 2.11, $\dim M \leq 4$. This implies $G = GL(2, 5)$ and $|g| = 8$, yielding the exceptional case in (2).

Thus, we may assume that $|g|$ divides $q - 1$. In this case, w.l.o.g. we may assume that $g \in T$, where T is the subgroup of diagonal matrices in G . As $\tau(G)/\tau(Z(G))$ is cyclic, items (1) and (2) of the statement follow from Lemma 4.2.

Since, by Lemma 4.1, every irreducible FG -module lifts to characteristic zero, the above results hold for any $\ell \neq 2$. So, from now on, we assume that $\ell = 2$, and hence q is odd.

Suppose that $\tau(g)$ is almost cyclic. The case where $\tau(g)$ is a transvection (recorded in item (3) of the statement) follows from Lemma 4.4. So we can assume that $g^2 \notin Z(G)$ (otherwise $\tau(g^2) = Id$, and hence $\tau(g)$ would be a transvection). This implies that g is reducible on the natural module of G , and hence $|g|$ divides $q - 1$. Indeed, assume that g is irreducible. Then g is contained in a cyclic subgroup X of $GL(2, q)$ of order $q^2 - 1$. As X contains the subgroup of scalar matrices (of order $q - 1$), the order of h divides $q + 1$. By assumption, $(q + 1)/2$ is odd, whence $g^2 \in Z(G)$, a contradiction.

Thus, we can assume that $g \in T$. We wish to use Lemma 4.2, which is stated in terms of ζ^T , where $\zeta \in \text{Irr } Z(G)$ is such that $\tau|_{Z(G)} = \zeta \cdot \text{Id}$.

Let $a = |T : SZ(G)|$, where S is the Sylow 2-subgroup of T . Set $\overline{G} = G/(S \cap (Z(G)))$ and let $\overline{S}, \overline{T}$ be the projections of S, T into \overline{G} . Then clearly $|\overline{T} : \overline{SZ(G)}| = a$. Let us view ζ^T as a representation of \overline{T} (clearly, $S \cap Z(G)$ is in the kernel of $\tau|_T$ as well as ζ^T). That is, let us express ζ^T as $\zeta_1^{\overline{T}}$, where ζ_1 is ζ viewed as a representation of $Z(G)/(S \cap Z(G))$. Then $\zeta_1^{\overline{T}}|_{\overline{S}} = a \cdot \rho_S^{reg}$.

Note that $h \in \overline{S} \subseteq \overline{T}$. If $\tau(g)$ is almost cyclic, then so is $\zeta_1^{\overline{T}}(h)$. By Clifford's theorem, this implies $a = 1$ and $|h| = |\overline{S}|$, and therefore $\zeta_1^{\overline{T}}(h) = \zeta^T(g)$ is represented by a Jordan block of size $|h|$.

Note that $a = 1$ means that $|T : Z(G)|$ is a 2-power. This implies that $G' = SL(2, q)$ has no 2-modular irreducible representation of degree $q + 1$. Indeed, by [3, 9.2], G' has no nilpotent block, and hence M belongs to the principal 2-block. Then the claim follows from [4]. In turn, this implies that case (4) of Lemma 4.2 does not occur. Indeed, suppose that $\dim M = q + 1$. Then $M|_{G'}$ is reducible. By Clifford's theorem, $M|_{G'} = M_1 \oplus M_2$, where M_1, M_2 are irreducible FG' -modules of dimension $(q + 1)/2$. However, $SL(2, q)$ has no irreducible 2-modular representation of such dimension (see [4]). This is a contradiction.

Furthermore, as $\ell = 2$, there are no irreducible F -representations of G of degree q (see [4]). Hence, case (5) of Lemma 4.2 does not occur.

Now, we apply Lemma 4.2. Suppose first that $G \subseteq Z \cdot SL(2, q)$. (Recall that Z is the group of scalar matrices in $GL(2, q)$.) Then (see the argument above) $\dim M \neq q + 1, (q + 1)/2$. Moreover, $\tau(g)$ is not almost cyclic in case (3), whereas it is so in case (1). So the lemma is true in this case. Next, suppose that G is not contained in $Z \cdot SL(2, q)$. Then, cases (1) and (2) of Lemma 4.2 are ruled out, whereas the matrix $\tau(g)$ is cyclic in case (3).

Lemma 4.6. *Let $J_n \in GL(n, 2)$, $n > 2$, be a Jordan block, where $2^{k-1} < n \leq 2^k$, $k > 1$. Then the Jordan normal form of $J_n^{2^{k-1}}$ is $\text{diag}(J_2, \dots, J_2, \text{Id}_{2^k-n})$.*

Proof. We argue by induction on k . Clearly, the statement is trivially true for $k = 2$, that is $n = 3, 4$.

By [9, Lemma 5.4], the Jordan form of J_n^2 is $\text{diag}(J_m, J_m)$ if $n = 2m$ is even, and $\text{diag}(J_{m+1}, J_m)$ if $n = 2m + 1$ is odd. To apply induction, we need the size s of each Jordan block of J_n^2 to satisfy the inequalities $2^{k-2} < s \leq 2^{k-1}$. If n is even, $2^{k-1} < n \leq 2^k$ implies $2^{k-2} < n/2 \leq 2^{k-1}$, as required. If n is odd, $n < 2^k$, so $\frac{n+1}{2} \leq 2^{k-1}$. Similarly, $2^{k-2} < \frac{n-1}{2}$, except when $n - 1 = 2^{k-1}$.

Suppose first that n is even. Then, by induction, the Jordan form of $J_{n/2}^{2^{k-2}}$ has $2^{k-1} - n/2$ trivial blocks. Hence the Jordan normal form of $J_n^{2^{k-1}}$ has exactly $2^{k-1} + 2^{k-1} - n = 2^k - n$ trivial blocks, as required.

Next, suppose that n is odd.

Suppose first that we are in the exceptional case where $n = 2^{k-1} + 1$. Then the Jordan form of J_n^2 is $\text{diag}(J_{m+1}, J_m) = \text{diag}(J_{2^{k-2}+1}, J_{2^{k-2}})$. It follows that $J_m^{2^{k-2}} = \text{Id}$, whereas $J_{m+1}^{2^{k-2}}$ is a transvection. Therefore, the Jordan form of $J_n^{2^{k-1}}$ is $\text{diag}(J_2, \text{Id}_{n-2})$, and hence $n - 2 = 2^{k-1} - 1 = 2^k - 2^{k-1} - 1 = 2^k - n$, as required.

In the general case, the Jordan form of $J_n^{2^{k-1}} = (\text{diag}(J_{m+1}, J_m))^{2^{k-2}}$ has $2^{k-1} - (m + 1) + (2^k - m) = 2^k - n$ trivial blocks, as required.

Note: A partial version of the result stated in the following Lemma is contained in a paper by Guralnick and Tiep ("Some bounds for H^2 ", in preparation). For the reader's convenience, we have written down a comprehensive proof.

Lemma 4.7. *Let $SL(2, q) \subseteq G \subseteq GL(2, q)$, where $q \equiv -1 \pmod{4}$. Let $g \in G$ be a 2-element such that $g^2 \notin Z(G)$, and let h be the projection of g into $\overline{G} := G/Z(G)$. For $\ell = 2$, let M be an irreducible FG -module of dimension $q - 1$ (respectively, $(q - 1)/2$), and let τ be the representation afforded by M . Then $\tau(g)$ is almost cyclic if and only if $q + 1$ is a 2-power (that is, q is a Mersenne prime), and $|h| = q + 1$ (respectively, $(q + 1)/2$).*

Proof. The "only if" part. Clearly, $G' = SL(2, q)$ and $\overline{G'} = PSL(2, q)$. Let $t \in \langle g \rangle$ be such that $t \notin Z(G)$, but $t^2 \in Z(G)$, and let \bar{t} be the projection of t into \overline{G} . Observe that $\bar{t} \in \overline{G'}$ (as $Z(GL(2, q)) \cdot SL(2, q)$ has index 2 in $GL(2, q)$, $g^2 \notin Z(G)$ and the index of G' in $Z(GL(2, q)) \cdot SL(2, q)$ is odd).

Set $t = g^{2^m}$, so that $\bar{t} = h^{2^m}$, and let D be the image in \overline{G} of the group of diagonal matrices in $SL(2, q)$. Then $|D| = (q - 1)/2$, which is odd. Note that $N_{\overline{G'}}(D)$ contains an involution inverting the elements of D . Since all the involutions of $\overline{G'}$ are conjugate to each other, we may assume that this inverting involution is \bar{t} . In addition, note that $C_D(\bar{t}) = 1$. Let $D = \langle d \rangle$. By Lemma 4.2, items (1), (3), there are $|d|$ distinct eigenspaces M_λ of d on M , where λ is an eigenvalue of d . As $|d|$ is odd, $\bar{t}(M_\lambda) = M_{\lambda^{-1}}$ and $\bar{t}(M_\lambda) = M_\lambda$ implies $\lambda = 1$. It follows that the Jordan form of \bar{t} on M is $\text{diag}(J_2, \dots, J_2, H)$, where H is the Jordan form of the matrix of \bar{t} on M_1 .

Moreover, by Lemma 4.2, $\dim M_1 = 2$ if $\dim M = q - 1$, whereas $\dim M_1 = 1$ if $\dim M = (q - 1)/2$. In the latter case $H = \text{Id}_1$. In the former case H is either J_2 or Id_2 . We show that $H = \text{Id}_2$ actually holds.

Suppose the contrary. Then the Jordan form of \bar{t} is $\text{diag}(J_2, \dots, J_2)$. Let K be the Jordan form of h on M . It follows from Lemma 4.6 that $K = \text{diag}(J_{2^{m+1}}, \dots, J_{2^{m+1}})$. As $(q - 1)/2$ is odd, this can only happen when $m = 0$, that is, $g = t$. However, this implies that $t^2 = g^2 \in Z(G)$, against our assumptions. Thus, $H = \text{Id}_2$.

It also follows from Lemma 4.6 that $K = \text{diag}(J_{2^{m+1}}, \dots, J_{2^{m+1}}, J_{2^{m+1}-2})$ or $K = \text{diag}(J_{2^{m+1}}, \dots, J_{2^{m+1}}, J_{2^{m+1}-1}, J_{2^{m+1}-1})$ (resp., $K = \text{diag}(J_{2^{m+1}}, \dots, J_{2^{m+1}}, J_{2^{m+1}-1})$). As K is supposed to be almost cyclic, we must have $K = J_{2^{m+1}-2}$ (resp., $K = J_{2^{m+1}-1}$). Therefore, $q - 1 = 2^{m+1} - 2$ (resp., $(q - 1)/2 = 2^{m+1} - 1$). So $q + 1$ is a 2-power, and $|h| = 2^{m+1} = q + 1$ (resp., $(q + 1)/2$), as claimed.

The "if" part. We are now given that $q + 1$ is a 2-power and $|h| = q + 1$ (resp., $(q + 1)/2$). Observe that the possible shapes of K given in the previous paragraph do not depend on the assumption that K is almost cyclic, but only on Lemma 4.6 and the assumption that $(q - 1)/2$ is odd. If $\dim M = q - 1$, then $|h| = 2^{m+1} = q + 1$, and hence the only option is $K = J_{2^{m+1}-2}$. Otherwise, $|h| = 2^{m+1} = (q + 1)/2$, and $K = J_{2^{m+1}-1}$.

Lemma 4.8. *Let $SL(2, q) \subseteq G \subseteq GL(2, q)$, where $q \equiv -1 \pmod{4}$. Let $g \in G$ be a non-central 2-element, and let h be the projection of g into $G/Z(G)$. Let M be an irreducible FG -module with $\dim M > 1$. Then g is almost cyclic on M if and only if:*

- (1) $\ell \neq 2$, $g \in SL(2, q) \cdot Z(GL(2, q))$, $\dim M = (q \pm 1)/2$ and $|h| = (q + 1)/2$;
- (2) $\ell \neq 2$, $g \notin SL(2, q) \cdot Z(GL(2, q))$, $\dim M = q$ or $q \pm 1$ and $|h| = q + 1$;
- (3) $\ell \neq 2$, $q = 7$, $\dim M = 3$ and $|h| = 2$.
- (4) $\ell = 2$, and one of the following holds:
 - i) $\dim M = q \pm 1$ and $|h| = q + 1$ (here the case $\dim M = q + 1$ only occurs for $g \notin SL(2, q) \cdot Z(GL(2, q))$);
 - ii) $\dim M = (q - 1)/2$ and $|h| = (q + 1)/2$.
 - iii) $q = 7$, $\dim M = 3$ and $|h| = 2$.

Additionally, in all the above cases q is a Mersenne prime.

Proof: Let τ be the representation of G afforded by M , and suppose that $\tau(g)$ is almost cyclic.

First of all, observe that, by the Remark preceding the statement of Lemma 4.5, we may assume that either $G = SL(2, q)$ or $G = GL(2, q)$. Recall that, by Lemma 4.1, every irreducible FG -module lifts to characteristic zero. Hence, if $\ell \neq 2$, it is enough to verify the lemma for $\ell = 0$, which can be done examining the character table of G . This yields items (1), (2) and (3) of the statement. (In (1), for $q = 7$, $|g| = 8$.)

So, from now on, we may assume that $\ell = 2$.

Suppose first that $g^2 \in Z(G)$. As $\ell = 2$, then $\tau(g)$ acts as a transvection on M . It follows that case (2) of Lemma 4.4 holds, and hence $G = SL(2, 7)$. In this case, $\dim M = 3$, $|g| = 4$ and $|h| = 2$, which gives item (4), iii) of the statement.

Thus, from now on we may assume that $g^2 \notin Z(G)$. Note that this implies that g is irreducible on the natural module of G (otherwise $|g|$ divides $q-1$, and hence $g^2 = 1$, as $(q-1)/2$ is odd by assumption).

It is well known that the irreducible 2-modular representations of $PSL(2, q)$ of non-zero defect are of degree 1, $q-1$ or $(q-1)/2$ (see [3]). Thus the case $G = SL(2, q)$, $\ell = 2$ is dealt with in Lemma 4.7, provided M has non-zero defect as a $PSL(2, q)$ -module. Now, recall that a Sylow 2-subgroup P of $PSL(2, q)$ is dihedral of order dividing $q+1$ (as $q \equiv -1 \pmod{4}$). So, we are left to examine the case where $\dim M = q+1$. Observe that $M|_P$ is a projective FP -module, and hence $M|_P = m \cdot \rho_P^{reg}$ for some integer $m > 0$. As $\tau(G) \cong PSL(2, q)$, we may assume that $\tau(g) \in P$. It follows that the matrix of $\tau(g)$ is not almost cyclic. Indeed, the Jordan form of the matrix of $\tau(g)$ consists of $d := m \cdot |P|/|\tau(g)|$ blocks of equal size. As P is not cyclic, $d > 1$.

By the above, we may now assume that $G = GL(2, q)$ (and $\ell = 2$). Set $G' = SL(2, q)$.

Note that $\dim M$ is not of degree q , $(q+1)/2$. Indeed suppose the contrary. Then, by Clifford's theorem, either $M|_{G'}$ is irreducible (which is not the case, e.g. see [4, pp. 90-91]), or $M|_{G'} = M_1 \oplus M_2$, where M_1, M_2 are irreducible FG' -modules of the same dimension. But this is impossible, considering the degrees of the irreducible FG' -modules. Next, suppose that $\dim M = q+1$. Then $M|_{G'}$ is irreducible, by similar reasons, and we may assume that either $\tau(g) \in P$ or $\tau(g^2) \in P$. In the former case $\tau(g)$ is not almost cyclic, as seen above. So, let $\tau(g) \notin P$. Then $\tau(g^2) \in P$, so the Jordan form of the matrix of $\tau(g^2)$ consists of $d := m \cdot |P|/|\tau(g^2)|$ blocks of equal size. It then follows that the Jordan form of the matrix of $\tau(g)$ consists of $d := m \cdot |P|/|\tau(g)|$ blocks of equal size, and hence is almost cyclic if and only if $m = 1$ and $|\tau(g)| = q+1$. This is part of item (3), *i*) in the statement of the Lemma.

Finally, we are left to examine the cases where $\dim M = q-1$ or $(q-1)/2$. These are dealt with in Lemma 4.7, and the results are stated in item (4), *i*) and *ii*) of the statement.

At this point, we are in a position to prove Theorem 1.2, stated in the Introduction:

Proof of Theorem 1.2. If $p > 2$, item (1) of the statement follows from Lemma 4.3. So, suppose that $p = 2$. We distinguish two cases, according to q being $\equiv 1 \pmod{4}$ or $\equiv -1 \pmod{4}$. If $q \equiv 1 \pmod{4}$, the claims in item (2) of the statement follow from Lemma 4.5. If $q \equiv -1 \pmod{4}$, the claims in item (2) of the statement follow from Lemma 4.8. Thus, the theorem is proven.

The following Lemma and its Corollary show that the results stated in Theorem 1.2 carry over to any group G such that $SU(2, q) \subseteq G \subseteq U(2, q)$.

Lemma 4.9. *Let $G = GL(2, q)$ and $H = U(2, q)$, for $q > 3$. Then there exists a group X such that $X = Z(X) \cdot G = Z(X) \cdot H$.*

Proof. Let us consider the groups G and H as naturally embedded subgroups of the algebraic group $\overline{G} = GL(2, \overline{F}_q)$. Recall that $G' \cong H'$. By the general theory of representations of Chevalley groups (see also [3], Chapter 10), G' and H' are conjugate in \overline{G} . So, up to taking a suitable conjugate of, say, G within \overline{G} , we may assume that $G' = H'$. Set $X = \langle G, H \rangle$, so that $X' = G' = H'$. Let $x \in X$, $g \in G'$. Then $xgx^{-1} \in G'$. Let T be a split torus in G' , which is a conjugate in G' of the group of diagonal matrices in $SL(2, q)$. Then xTx^{-1} is another split torus, and it is conjugate to T in G' (as split tori are conjugate). So we can assume that $xTx^{-1} = T$. It is then easy to check that x is of shape $\text{diag}(a, b)$ or $\begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix}$, where $a, b \in \overline{F}_q$. Take $g = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Then xgx^{-1} equals $\pm \begin{pmatrix} 0 & b^{-1}a \\ -ba^{-1} & 0 \end{pmatrix} \in G'$ in both cases. Therefore, $b \in aF_q$, so $x \in Z \cdot GL(2, q)$, where z is a scalar matrix. This shows that $X = Z(X) \cdot G$. Next, we show that $X = Z(X) \cdot H$. Suppose first that q is even. Then $G = Z(G)G'$, whence, as $Z(G)$ and $Z(H)$ are both contained in $Z(X)$, $X = Z(X)G' = Z(X)H' = Z(X) \cdot H$, as claimed. Next, suppose that q is odd.

Then $G \not\subseteq Z(X) \cdot G'$. Indeed, let $g \in G$, with $\det(g)$ a non-square in F_q , and assume that $g = zg'$, where $z = \text{diag}(x, x)$, $x \in \overline{F}_q$, and $g' \in G'$. Then $x \in F_q$ and $\det(zg') = x^2$, a contradiction. It follows that $|G : Z(G)G'| = 2$, whence also $|X : Z(X)G'| = 2$ (as $X = Z(X)G$). Since $G' = H'$, it now suffices to show that H is not in $Z(X)G'$. For this, observe that the latter group has a non-trivial complex representation of degree $(q-1)/2$, whereas H does not, unless $q = 3$ (e.g. see [14]).

Corollary 4.10. *Let ρ be an irreducible representation of $H = U(2, q)$. Then ρ extends to X . Moreover, if $h \in H$ then there exists $g \in G = GL(2, q)$ such that $\rho(h) = \lambda\rho(g)$, where $\lambda \in F$. In addition, if $h^k \in Z(U(2, q))$ then $g^k \in Z(GL(2, q))$, that is, the order of g, h modulo centres are the same.*

The following results will be needed for the proof of Proposition 5.13 in Section 5.

Lemma 4.11. *Let $G = SL(n, q)$, where $(n, q) \in \{(3, 2), (3, 4), (4, 2)\}$. Let g be a semisimple element of G of p -power order, p a prime, and let M be an irreducible FG -module with $\dim M > 1$, on which the matrix of g is almost cyclic. Then one of the following holds:*

- (1) $G = SL(3, 2)$, and either $|g| = 7$ and M is arbitrary, or $|g| = 3$ and $\dim M = 3$.
- (2) $G = SL(4, 2)$, $|g| \in \{3, 5, 7\}$ and $\dim M = 7$. (Here, if $|g| = 3$, then g belongs to the class 3A, in the Atlas notation).

Proof. If $(|g|, \ell) = 1$, then the result follows by inspection of the Brauer characters of G (see [29]). Therefore, we may assume that ℓ divides $|g|$.

(1) Let $G = SL(3, 2)$. If $|g| = \ell = 7$ then, as $SL(3, 2) \cong PSL(2, 7)$, M is realized as a $PSL(2, 7)$ -module, and the result follows from the well known fact that a unipotent element $g \neq 1$ of $SL(2, \ell)$ in every irreducible representation of this group in characteristic ℓ is represented by a single Jordan block, and hence the matrix of g is cyclic. So, let $|g| = 3$. Then $\dim M \in \{3, 6, 7\}$. Thus, by Lemma 2.13 and Corollary 2.14, $\dim M = 3$.

(2) Let $G = SL(4, 2)$. In this case $|g| \in \{3, 5, 7\}$, and, for $p > 3$, the Sylow p -subgroups S of G are cyclic of order p .

First, let $\ell = p = 7$. Then the minimum dimension of M equals 7 (see [29]), in which case M has defect zero. It follows from Lemma 2.13 that the matrix of g on M is a single Jordan block, and hence cyclic. Otherwise, M has defect 1. In this case, as $N_G(S)/S$ is abelian, it follows from Corollary 2.14 that $\dim M \leq 8$. However, for $\ell = 7$ the only irreducible F -representation of dimension at most 8 is that of dimension 7, a contradiction.

Next, let $\ell = p = 5$. Then g is regular; hence, by Lemma 2.8, G can be generated by three suitable conjugates of g . By Lemma 2.11, $\dim M \leq 12$. As G has no irreducible F -representation of degree d for $7 < d < 13$ (see [29]), it follows that $\dim M = 7$. The same is true for $p = 3$. Indeed, by Proposition 2.10, G can be generated by at most 4 conjugates of g ; this implies $\dim M \leq 8$, by Lemma 2.11. It follows that $\dim M = 7$ (see [29]).

Now, for both $p = 3$ and $p = 5$, there is a unique FG -module of dimension 7. It follows that M is isomorphic to the only non-trivial constituent of the 8-dimensional permutation module for the alternating group $A_8 \cong SL(4, 2)$. For $p = 5$, this implies that g is almost cyclic on M . So, let $p = 3$. There are exactly two conjugacy classes of elements of order three in G , labelled 3A and 3B in [5]. The class 3A is represented by a permutation fixing 5 out of 8 points. It follows that $g \in 3A$ is almost cyclic on M . Next, suppose that $g \in 3B$. Then g is contained in a subgroup $X \cong A_7$, and $M|_X$ contains a non-trivial 6-dimensional constituent N , say, which is also a constituent of the 7-dimensional permutation module for A_7 . We claim that g is not almost cyclic on M , and for this it suffices to show that g is not almost cyclic on N . Suppose the contrary. Observe that X can be generated by two suitable elements from 3B (direct computation using GAP). It then follows from Lemma 2.11 that an irreducible constituent of N must have dimension ≤ 4 . However, the

minimal dimension of a non-trivial 3-modular representation of A_7 equals 6. This yields a contradiction.

(3) Let $G = SL(3, 4)$. Here $p \in \{3, 5, 7\}$, and the Sylow 5- and 7-subgroups S of G are cyclic of prime order. Moreover, $N_G(S)/S$ is abelian. Let first $p = \ell = 5$. If M has defect zero, then $\dim M \geq 15$, and hence g is not almost cyclic on M by Lemma 2.11. Otherwise, by Corollary 2.14, g almost cyclic implies $\dim M \leq 6$. However, G has no non-trivial F -representations of such degrees. Now, let $p = \ell = 7$. If M has defect zero, then $\dim M \geq 21$, and again g is not almost cyclic on M by Lemma 2.11. Otherwise, by Corollary 2.14, g almost cyclic implies $\dim M \leq 8$. Again, G has no non-trivial F -representations of such degrees. Finally, let $p = \ell = 3$. In this case, it suffices to deal with the group $H = PSL(3, 4)$. Let h be the projection of g into H . Then $|h| = 3$, and by Proposition 2.10 H is generated by three suitable conjugates of h . Hence $\dim M \leq 6$, by Lemma 2.11. But again, there is no 3-modular irreducible representation of H of this degree. (Note, however, that the universal covering of G has irreducible 5-modular representations of degree 6, as well as irreducible 7-modular representations of degree 6 and 8, and g is almost cyclic on these modules, by Lemma 2.13).

Remark: Observe that the representation of $SL(3, 2)$ afforded by the FG -module M , where $\dim M = 3$, is *not* Weil, according to our definitions (see above).

Lemma 4.12. *Let $SL(n, q) \subseteq G \subseteq GL(n, q)$, where $n > 2$ and $(n, q) \neq (3, 3), (4, 3)$, and let $g \in G$ be a non-scalar semisimple element of p -power order, p a prime. Suppose that g stabilizes a 1-dimensional subspace on the natural module of G . Let M be an irreducible FG -module with $\dim M > 1$, affording the representation ϕ . Then $\phi(g)$ is not almost cyclic, unless one of the following holds:*

- (1) $G = SL(3, 2)$, $|g| = 3$ and $\dim M = 3$.
- (2) $G = SL(4, 2)$, $|g| \in \{3, 7\}$, where $g \in 3A$ if $|g| = 3$, and $\dim M = 7$.

Proof. Suppose that $\phi(g)$ is almost cyclic, and assume that $g \in P$, where P is the stabilizer of a 1-dimensional subspace. Let U be the unipotent radical of P , and let τ be an irreducible constituent of $\phi|_P$ non-trivial on U . Note that τ is faithful on U : indeed, any subgroup W of U on which $\tau_W = Id$, would be normalized by P ; however, P acts transitively on $U \setminus \{1\}$ by conjugation. Let T be the FP -module afforded by τ . Then $T|_U = \bigoplus T_\kappa$, where κ runs over the group K of F -characters of U , and $T_\kappa = \{t \in T \mid ut = \kappa(u)t, \forall u \in U\}$. Moreover, the action of P on U by conjugation is dual to the action of P on K . Let $h = g^s \notin Z(G)$, where s is such that $h^p \in Z(G)$ (so $g^{ps} \in Z(G)$). Let $\phi(g^{ps}) = \lambda \cdot Id$. It is straightforward to check that $[h, U] \neq 1$. As U acts scalarly on every T_κ , there is κ such that $T_\kappa \neq 0$ and $hT_\kappa \neq T_\kappa$ (otherwise $\tau([h, U]) = 1$, and hence $[h, U] = 1$ as $\tau(U) \cong U$). It follows that the g -orbit containing this κ is of size ps . Set $d := \dim T_\kappa$ and $R = \bigoplus_{\nu \in \{g^i \kappa\}} T_\nu$. If $p = \ell$, then the matrix of g on R is similar to the sum of d Jordan blocks J_{ps} . If $p \neq \ell$, then all the ps -roots of λ are eigenvalues of $\tau(g)$, each with multiplicity at least $\dim T_\kappa$. Therefore, $d = 1$, since $\phi(g)$ is assumed to be almost cyclic. Furthermore, observe that, if τ' is another irreducible constituent of $\phi|_P$ non-trivial on U , then we reach the same conclusion. As $\phi(g)$ is assumed to be almost cyclic, we conclude that τ is the only irreducible constituent of $\phi|_P$ non-trivial on U . It follows that $T' := \bigoplus_{\kappa \in K \setminus \{1_U\}} T_\kappa$ must be an irreducible FP -module of dimension at most $|K| - 1 = |U| - 1 = q^{n-1} - 1$.

Now, let T_1 denote the subspace T_κ with $\kappa = 1_U$. Clearly, T_1 can be viewed as an $F(P/U)$ -module, and by the above $M|_P = T' \oplus T_1$, where T' is irreducible. Observe that $L := P/U$ is isomorphic to a subgroup of the group $X := GL(n-1, q) \times GL(1, q)$ containing $SL(n-1, q)$. As $X/Z(X) \cong PGL(n-1, q)$, it follows that every normal subgroup of L either is contained in $Z(L)$, or it contains $L' \cong SL(n-1, q)$, unless $(n-1, q) = (2, 2), (2, 3)$. These exceptions, however, do not occur here, as $(n, q) \neq (3, 2)$ by Lemma 4.11 and $(n, q) \neq (3, 3)$ by assumption.

It was shown in [38, p.237], that $P \cap SL(n, q)$ has an irreducible constituent on T_1 of dimension greater than 1, unless $(n, q) \in \{(4, 2), (3, 2), (4, 3), (3, 4)\}$. Observe that the exceptional cases where $(n, q) \in \{(4, 2), (3, 2), (3, 4)\}$ were dealt with in Lemma 4.11, yielding items (1) and (2) of the statement, whereas the case $(n, q) = (4, 3)$ is ruled out by assumption. Therefore, from now on, we may suppose that $P \cap SL(n, q)$ has an irreducible constituent on T_1 of dimension greater than 1. As $U \subset SL(n, q)$, it follows that P , and hence L , has an irreducible constituent on T_1 of dimension greater than 1.

Observe that, since g is almost cyclic on M , g must act scalarly on T_1 . [Otherwise, g would have either a non-trivial Jordan block on T_1 (if $\ell = p$), or at least 2 distinct eigenvalues on T_1 , which are also ps -roots of λ (if $\ell \neq p$). But this would contradict the almost cyclicity of g on M , in view of the action of g on T' , as described above.] So, we may suppose that g acts on T_1 scalarly, and hence that $\rho(g)$ is scalar. Let $N = \{a \in L : \rho(a) \text{ is scalar}\}$. Clearly, N is a normal subgroup of L . So, either $N \subseteq Z(L)$ or N contains L' . The latter cannot happen, as L/L' is abelian, and hence ρ would be one-dimensional, which is false. So $N \subseteq Z(L)$, and hence $g \bmod U \in Z(L)$. Let us consider the action of P , and hence of L , on U by conjugation. Then, viewing U as a vector space over F_q , $Z(L)$ acts on U scalarly, and the kernel of the action of L is $Z(G)$. It readily follows that all the g -orbits on U , but one, have the same size $ps > 1$, and the number of non-trivial g -orbits is at least $(q^{n-1} - 1)/(q - 1) > 1$. Clearly, this remains true for the action of g on K . However, as shown above, g must have only one non-trivial orbit on K , which gives a contradiction.

In the next two Lemmas we deal with the cases where $(n, q) \in \{(3, 3), (4, 3)\}$, which were left open in Lemma 4.12.

Lemma 4.13. *Let $SL(3, 3) \subseteq G \subseteq GL(3, 3)$, and let $g \in G$ be a non-scalar semisimple element of p -power order, for some prime p . Let M be an irreducible FG -module with $\dim M > 1$, affording a representation ϕ . Then the matrix of g on M is not almost cyclic, unless one of the following holds:*

- (1) $\ell \neq 2, 13$, $|g| = 13$ and $\dim M = 12$ or 13 (in which cases g is cyclic on M);
- (2) $\ell = 2$, $|g| = 13$ and $\dim M = 12$ (in which case g is cyclic on M);
- (3) $\ell = p = 13$, $|g| = 13$ and $\dim M = 13$ (in which case g is cyclic on M);
- (4) $\ell = p = 13$, $|g| = 13$ and $\dim M = 11$ (in which case g is cyclic on M).

Proof. Observe that, since $GL(3, 3) = SL(3, 3) \times \{\pm \text{Id}\}$, we may assume that $G = SL(3, 3)$. Here $p \in \{2, 13\}$. Suppose first that $p = 13$. If $\ell \neq 2, 13$ or $\ell = 2$, then items (1) and (2) of the statement follow by direct inspection of the character table of G and [29], respectively. So, suppose that $\ell = p = 13$. If M has defect zero, then $\dim M \in \{13, 26, 39\}$. Hence g is almost cyclic on M precisely when $\dim M = 13$, by Lemma 2.13. If M has positive defect, then $\dim M \in \{11, 16\}$. As $N_G(\langle g \rangle)/\langle g \rangle$ is abelian, Corollary 2.14 rules out the case $\dim M = 16$, while direct computation using MAGMA shows that g is cyclic on M when $\dim M = 11$. This gives items (3) and (4) of the statement.

Next, suppose that $p = 2$. If $\ell \neq 2$, then the statement follows by inspection of the character table of G and [29]. So, let $\ell = 2$. If g is an involution, then the claim follows from Lemma 2.12 (as $\phi(G)$ is not generated by transvections). Suppose that $g^2 \neq 1$. Then one observes that $C_G(g)$ contains no element of order 3, that is, g is regular. By Lemma 2.8, G is generated by three conjugates of g . Then $\dim M \leq 3(|g| - 1)$ by Lemma 2.11. As the minimum dimension of a non-trivial F -representation of G is 12, it follows that $|g| = 8$, and $\dim M \leq 21$. So $\dim M \in \{12, 16\}$ (see [29]). As the order of a Sylow 2-subgroup S of G is 16, the representations of degree 16 are of defect zero, and hence $\phi|_S = \rho_S^{\text{reg}}$, by Lemma 2.13. It follows that $\phi(g)$ is not almost cyclic. If M has dimension 12, then the claim follows by direct computation, using MAGMA.

Lemma 4.14. *Let $SL(4, 3) \subseteq G \subseteq GL(4, 3)$, and let $g \in G$ be a non-scalar semisimple element of p -power order, for some prime p . Let M be an irreducible FG -module with $\dim M > 1$. Then the matrix of g on M is not almost cyclic.*

Proof. By way of contradiction, assume that the matrix of g is almost cyclic on M . Recall that the minimum dimension of a (projective) irreducible F -representation of G is 26. Suppose first that $p > 2$. Then $p \in \{5, 13\}$. As $|G/G'| \leq 2$, it suffices to verify the lemma for $G = SL(4, 3)$. (Indeed, we may assume that $g \in G'$. Moreover, as g is almost cyclic on M , g must be almost cyclic on any constituent of $M|_{G'}$.) Observe that g is regular. For $p = 5$, it follows from Lemma 2.8 and Lemma 2.11 that $\dim M \leq 12$, which is a contradiction. So, let $p = 13$. Then, by Lemma 2.8 and Lemma 2.11, $\dim M = 26$. If $\ell \neq 13$, a direct inspection of the character table and the Brauer characters of G in [5] and [29] shows that g is not almost cyclic on M . If $\ell = 13$, then M has defect zero, and hence g is not almost cyclic on M by Lemma 2.13.

Next, let $p = 2$, and let V be the natural module for G . Note that $g^8 \in Z(G)$. (Indeed, if g is irreducible, then $|g| \leq 16$, and hence $g^8 = \pm \text{Id}$. On the other hand, if g is reducible, then $|g| \leq 8$.) If g is regular (that is, $C_G(g)$ contains no unipotent element), then g is generated by three conjugates of g , by Lemma 2.8. But then $\dim M \leq 21$ by Lemma 2.11, a contradiction. So, suppose that g is not regular. Then g is reducible (by Schur's Lemma), and hence $|g| \leq 8$. If $g^4 \in Z(G)$, then, by Proposition 2.10(1), G is generated by four suitable conjugates of g . Hence $\dim M \leq 12$ by Lemma 2.11, again a contradiction. So, we may assume that $|g| = 8$. Then $V = V_1 \oplus V_2$ (a direct sum decomposition), where $\dim V_i = 2$ and $gV_i = V_i$ for $i = 1, 2$. Set $g_i = g|_{V_i}$. If both g_1, g_2 are of order 8, then $g^4 \in Z(G)$, which case has been already ruled out. So we may assume that $|g_1| = 8$ and $|g_2| \leq 4$. Then g_1 is irreducible on V_1 , and hence both the eigenvalues of g_1 on $V_1 \otimes \overline{F}_q$ are primitive 8-roots of unity. As g is not regular, it follows that the eigenvalues of g_2 on $V_2 \otimes \overline{F}_q$ are not distinct, whence $g_2 = \pm \text{Id}$. So g stabilizes a direct sum decomposition of V , say $V = W \oplus U$, where $\dim W = 1$. Let H denote the stabilizer in G of both W and U , so that $g \in H$. If $G = SL(4, 3)$, then $H \cong GL(3, 3)$, whereas if $G = GL(4, 3)$, then $H \cong GL(3, 3) \times Y$, where $Y = \{\pm 1\}$. As $g \in H$, the result follows from Lemma 4.13.

Lemma 4.15. *Let $G = Sp(4, 3)$, and $g \in G$ be a non-scalar semisimple element of p -power order, p a prime. Let ϕ be an irreducible F -representation of G . Then the matrix $\phi(g)$ is almost cyclic if and only if one of the following holds:*

- (1) $p = 2$, $\ell \neq 2$ and
 - (i) $|g| = 2$ and $\dim \phi = 5$;
 - (ii) $|g| = 4$, $g^2 \notin Z(G)$ and $\dim \phi = 4$;
 - (iii) $|g| = 8$, $g^4 \in Z(G)$ and $\dim \phi = 4$ or 5.

Furthermore, the matrix of $\phi(g)$ is cyclic only if $|g| = 8$ and $\dim \phi = 4$.

- (2) $p = 5$ and $\dim \phi \in \{4, 5, 6\}$, where $\dim \phi \neq 6$ if $\ell = 3$ and $\dim \phi \neq 5$ if $\ell = 2$. Furthermore, ϕ is faithful if and only if $\dim \phi = 4$ and $\ell \neq 2$.

- (3) $p = \ell = 2$ and $\dim \phi = 4$. In addition, either $|g| = 4$, or $|g| = 2$ and $\phi(g)$ is a transvection in $SU(4, 2)$.

Proof. First, let $p > 2$. Note that a Sylow 5-subgroup S of G is of order 5, and we may assume $g \in S$. If $\ell \neq 5$, then the claim in (2) follows from a direct inspection of the Brauer character tables of G in [29].

So, let $\ell = 5$. Observe that $C_G(g)$ has order 10, and hence g is regular. It follows that $\dim \phi \leq 12$, by Lemmas 2.8 and 2.11. Thus $\dim \phi \in \{4, 5, 6, 10\}$. If $\dim \phi = 5$ or 10, then ϕ is of 5-defect zero, and hence by Lemma 2.8 $\phi|_S = \rho_S^{\text{reg}}$ or $2\rho_S^{\text{reg}}$, respectively. Therefore, the matrix of g is almost cyclic (in fact cyclic, represented by a single Jordan block J_5) only when $\dim \phi = 5$. If $\dim \phi \in \{4, 6\}$, then direct computation using MAGMA shows that $\phi(g)$ is cyclic, yielding (2).

Next, let $p = 2$ and $\ell \neq 2$. In this case the claim in (1) follows by direct computation from the data in [5] and [29].

If $p = \ell = 2$, then ϕ can be viewed as a representation of $SU(4, 2)$. It is easy to check, using MAGMA, that in both the classes 4A and 4B (Atlas notation) can be found two suitable elements generating $SU(4, 2)$, and hence, for g in these classes, we only need to examine $\phi(g)$ for $\dim \phi \leq 6$. It turns out that $\phi(g)$ is almost cyclic only when $\dim \phi = 4$

(almost cyclic in case 4A, cyclic in case 4B). Finally, if $|g| = 2$, almost cyclicity only occurs when g is a transvection, in which case five conjugates of g are enough to generate the group. This gives (3).

Remark. Recall that $O^-(6, 2) = SO^-(6, 2) \cong SU(4, 2) \cdot C_2$. The group $O^-(6, 2)$ is generated by transvections, and has an irreducible representation of degree 6 over the complex numbers, in which there exists an element of order 2 represented by an almost cyclic matrix (it belongs to the class $2C$ in the notation of [5]). (Of course, there are no transvections in the commutator subgroup of $O^-(6, 2)$). In addition, $O^-(6, 2) \cong CSp(4, 3)$, the conformal symplectic group (see [5, p. 26]), and $|\text{Aut } G : G| = 2$.

Lemma 4.16. *Let $G = SU(4, 2)$. Let $g \in G$ be a non-scalar semisimple element of p -power order, p a prime. Let ϕ be an irreducible F -representation of G such that the matrix $\phi(g)$ is almost cyclic. Then one of the following holds (we use the Atlas notation for conjugacy classes):*

- (1) $p = 3, \ell \neq 3, |g| = 3, g \in 3D$ and $\dim \phi = 5$, or $g \in 3C$ and $\dim \phi = 6$;
- (2) $p = 3, \ell \neq 3, |g| = 9, g \in 9A, 9B$ and $\dim \phi = 5, 6$;
- (3) $p = 3, \ell = 3, |g| = 3, g \in 3C, 3D$ and $\dim \phi = 5$;
- (4) $p = 3, \ell = 3, |g| = 9, g \in 9A, 9B$ and $\dim \phi = 5$;
- (5) $p = 5$ and $\dim \phi = 5, 6$.

Proof. Note that $G \cong PSp(4, 3)$. If $p = 3$ and $\ell \neq 3$, then (1) follows from [10, Lemma 4.2], where the reader can find more details.

Now, let $p = \ell = 3$. All the 3-modular irreducible representations of $PSp(4, 3)$ are available on the Atlas on line. Easy routines using the MAGMA package yield the results listed in (3) and (4).

Finally, let $p = 5$. Then the claim in (5) follows from Lemma 4.15.

Lemma 4.17. *Let $G = SU(5, 2)$. Let $g \in G$ be a non-scalar semisimple element of p -power order, p a prime. Let ϕ be an irreducible F -representation of G . Then the matrix $\phi(g)$ is almost cyclic if and only if one of the following occurs:*

- (1) $p = 3, \ell \neq 3, |g| = 9, g \in 9C, 9D$ and $\dim \phi = 10$;
- (2) $p = 11$ and $|g| = 11$ and $\dim \phi = 10$ or 11 .

(Note that the representations occurring in (1) and (2) are Weil F -representations of G).

Proof. First, observe that, by Proposition 2.9, (1), G can be generated by at most five conjugates of g . By Lemma 2.11, this implies that, whenever $|g| = 3, 5, 9$, we only need to examine the F -representations ϕ of G of degree 10 and 11 (since any other irreducible F -representation of G has degree ≥ 43). On the other hand, the same holds when $|g| = 11$; indeed, using the MAGMA package, it turns out that, for $|g| = 11$, two suitable conjugates of g are enough to generate G . Then the statement follows by direct computation using the Atlas and the MAGMA package. (Note that in item (1), for $\ell = 3$, $\phi(g)$ has Jordan form $\text{diag}(J_8, J_2)$).

We close this Section with the following result, which will be needed in the sequel (see the proof of Lemma 2.11).

Lemma 4.18. *Let $G = U(6, 2)$ and let $g \in G$ be an element of order 9. Let τ be an irreducible F -representation of G . Then $\tau(g)$ is not almost cyclic.*

Proof. Let V be the natural module for G . Suppose first that g is not contained in any proper parabolic subgroup of G ; so, in particular, g is regular. Observe that g stabilizes a 3-dimensional subspace, obviously non-degenerate. One readily observes that there exists an orthogonal basis of V with respect to which g has one of the following shapes (where ε is a non-trivial cubic root of 1):

$$g_1 = \text{diag} \left(\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \varepsilon & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \varepsilon^2 & 0 & 0 \end{pmatrix} \right) \text{ or } g_2 = \text{diag} \left(\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \varepsilon^i & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & \varepsilon & 0 \\ 0 & 0 & \varepsilon^2 \end{pmatrix} \right)$$

for $i = 1, 2$ (but the matrices with $i = 1, 2$ only differ by a scalar, so we may assume $i = 1$). Note that $g_1 \in G' = SU(6, 2)$, whereas $\det g_2 \neq 1$; however, $g_2 \in G'$ up to a scalar.

Suppose first that $g = g_1$. By Lemma 2.7, given a semisimple element $x \in G'$ there are two conjugates of g whose product is equal to x . So, if we fix some element x of order 11 in G' , we can assume that $x = gg'$, where g' is conjugate to g . We claim that g and g' generate G' . Indeed, suppose the contrary. It suffices to show that g and g' are not contained in any maximal subgroup of G' . Inspecting the list of maximal subgroups M of $G'/Z(G')$ (see [5]), we observe that 11 is coprime to the order of any such M , except for the case where $M \cong SU(5, 2)$. Let $M_1 \cong U(5, 2)$ be the preimage of M in G' . Then M_1 (up to conjugacy) is the unique maximal proper subgroup of G' of order divisible by 11. So we may assume that $x, g, g' \in M_1$. Now, M_1 fixes a 1-dimensional subspace of V , whereas $g = g_1$ does not fix any such subspace, since it has no eigenvalues on V . This is a contradiction. Thus, $G = \langle g, g' \rangle$. By Lemma 2.11, $\dim \tau \leq 16$. However, the minimum dimension of a non-trivial irreducible F -representation of G' equals 21. This completes the analysis of this case.

Next, suppose that $g = g_2$. Since $|G : G'| = 3$, $G = \langle g, G' \rangle$. Using the MAGMA package, one sees that there is a conjugate g' of g such that $\langle g, g' \rangle = \langle g, G' \rangle = G$. As above, $\dim \tau \leq 16$ by Lemma 2.11. So we have again a contradiction, as in the previous paragraph.

Now, suppose that g is not regular. Then g is conjugate to an element g_3 of shape

$$g_3 = \text{diag} \left(\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \varepsilon^i & 0 & 0 \end{pmatrix}, \begin{pmatrix} \varepsilon_1 & 0 & 0 \\ 0 & \varepsilon_2 & 0 \\ 0 & 0 & \varepsilon_3 \end{pmatrix} \right),$$

where $\varepsilon_1, \varepsilon_2, \varepsilon_3$ are 3-roots of unity, not all distinct (corresponding to the 20 classes of non-regular elements of order 9 contained in G). It follows that g is contained in a parabolic subgroup P , say, which stabilizes an isotropic 1-dimensional subspace. Let U be the unipotent radical of P . Then $U/Z(U)$ is an elementary abelian 2-group of order $4^4 = 2^8$. Set $X = \langle g, U \rangle$, and let ϕ be an irreducible constituent of $\tau|_X$ non-trivial on $Z(U)$. Set $E = \phi(U)$. Then E is a group of symplectic type, and $E/Z(E) \cong U/Z(U)$ has order 2^8 (see [8]). However, Lemma 3.7 implies that $|g| = 2^4 \pm 1$, which is false, as $|g| = 9$.

5. ALMOST CYCLIC ELEMENTS IN WEIL REPRESENTATIONS

As mentioned in the Introduction, most non-trivial examples of almost cyclic matrices seem to arise in Weil representations of finite classical groups. In this Section we fully analyze such representations, with the aim of providing an exhaustive picture of the occurrence of almost cyclic matrices.

The use of induction is an essential part of our machinery. As we deal with classical groups, the starting point of induction will be the study of elements that are orthogonally indecomposable on the underlying vector space. This means that g is an element of a finite classical group G which does not stabilize any non-trivial non-degenerate subspace of V , where V is the natural module of G (in the case of $G = GL(n, q)$ or $SL(n, q)$ the word ‘non-degenerate’ must be dropped). This implies that one of two situations holds: either g is irreducible, or $G \neq GL(n, q), SL(n, q)$ and $V = V_1 \oplus V_2$, where V_1, V_2 are g -stable totally singular subspaces of V (e.g. see [25, Satz 1 and 2]). The orthogonally indecomposable case will be dealt with in Subsection 5.2. Next, the case where the element g is orthogonally decomposable must be treated. This will be done in Subsection 5.3.

5.1. Weil representations. We recall the notion and the basic properties of Weil representations.

Let E be an extraspecial r -group. If r is odd, assume E to be of exponent r . As always in this paper, F is an algebraically closed field of characteristic $\ell \neq r$, and F_q is a field of order q , where q is an r -power. It is well known that E has faithful irreducible F -representations, all of them of degree r^m , where $|E/Z(E)| = r^{2m}$. Let us single out

one of these representations and identify E with its image. Thus, E is now an irreducible subgroup of $GL(r^m, F)$. The commutator map $(a, b) \rightarrow [a, b]$ yields a symplectic space structure on $V := E/Z(E)$. Let N be the normalizer of E in $GL(r^m, F)$. Then the conjugation action of N on E preserves the commutation in E , and hence yields a homomorphism $\eta : N \rightarrow Sp(V)$, which is known to be surjective. This means that $E/Z(E)$ is isomorphic to the natural module for $Sp(V)$. Now let G be a non-trivial group. Suppose that there is an injective homomorphism $j : G \rightarrow N$ such that $j(G) \cap E = 1$. Then j yields a representation $G \rightarrow GL(r^m, F)$, which is called a *generic Weil representation*, and whose irreducible constituents are called *Weil representations* of G . In practice, it is not reasonable to use this definition for an arbitrary group G ; so we assume that $\eta(j(G))$ stabilizes no non-zero subspace of V . Thus the groups $Sp(2m, r)$ (r odd), $SU(m, r)$, $U(m, r)$, and $SL(m, r)$, $GL(m, r)$ are examples of the group G in question (e.g., see [16]).

In principle, a Weil representation of a group G as defined above depends on a faithful representation of E and on the embedding j . However, if $G \in \{SL(m, r), SU(m, r)\}$, there is in fact only one (up to equivalence) generic Weil representation, whereas if $G = Sp(2m, r)$, exactly two non-equivalent generic Weil representations can be obtained in this way. If $G \in \{GL(m, r), U(m, r)\}$, one obtains several generic Weil representations, but all of them differ from each other by tensoring with a one-dimensional representation of G (e.g., see [16]). In fact, this is immaterial for our purposes.

Additionally, we emphasize that every generic Weil representation of $G = GL(m, r)$ is the tensor product of the permutation F -representation of G , associated with the action of G on the vectors of the standard $F_r G$ -module, with a 1-dimensional module.

Now, let $m = nk$ and set $q = r^k$, $k \geq 1$. It is well known that there are embeddings $GL(n, q) \rightarrow GL(m, r)$, $Sp(2n, q) \rightarrow Sp(2m, r)$ and $U(n, q) \rightarrow Sp(2m, r)$ obtained by viewing F_q or F_{q^2} as vector spaces over F_r . We call them standard embeddings. Composing each of these embeddings with a representation j as defined above, one obtains generic Weil representations of these groups, and again, the above comments remain valid by replacing r by q . Namely, in this way one obtains exactly one generic Weil representation for $SL(n, q)$ and $SU(n, q)$ (up to equivalence), and exactly two generic Weil representations for $Sp(2n, q)$ (up to equivalence). Likewise, those for $GL(n, q)$ and $U(n, q)$ can be obtained from each other by tensoring with a one-dimensional one.

In this section we also use the term Weil character referring to the character (Brauer character) of the FG -module afforded by a Weil representation of G . It follows from the construction of a generic Weil representation that its Brauer character (when the characteristic ℓ of the ground field is prime) coincides with the restriction to ℓ' -elements of the Weil character in characteristic 0. One can refer to [16] and [50] for more details on the basic properties of Weil representations.

Each of the two ordinary (i.e. $\ell = 0$) generic Weil representations ϕ of $Sp(2n, q)$, q odd, has two irreducible constituents, ϕ^+, ϕ^- , say, of dimension $(q^n + 1)/2, (q^n - 1)/2$, respectively. They remain irreducible under reduction to any characteristic $\ell > 2$ coprime to q . For $\ell = 2$ this is only true for ϕ^- , while the reduction of $\phi^+ \bmod 2$ has two composition factors, one of them one-dimensional (and in fact trivial unless $(n, q) = (1, 3)$), the other one equivalent to $\phi^- \bmod 2$ (see [50]).

As mentioned above, up to tensoring by a one-dimensional representation, there is a unique ordinary generic Weil representation of $U(n, q)$; if $n > 2$, it consists of $q + 1$ composition factors, not equivalent to each other. If n is odd, then the dimensions of the irreducible constituents are $-1 + \frac{q^n + 1}{q + 1} = \frac{q^n - q}{q + 1}$ or $\frac{q^n + 1}{q + 1}$. If n is even, then the dimensions of the irreducible constituents are $\frac{q^n - 1}{q + 1}$ or $1 + \frac{q^n - 1}{q + 1} = \frac{q^n + q}{q + 1}$. These irreducible constituents remain irreducible and pairwise non-equivalent under restriction to $SU(n, q)$. The representations of lower degree remain irreducible under reduction modulo any prime ℓ coprime to q . The other representations remain irreducible provided $(\ell, q + 1) = 1$. More precisely, if $(\ell, q + 1) \neq 1$, the following holds (see [23, Proposition 9].) Assume first that n

is odd, and ψ , say, is an ordinary irreducible Weil representation of degree $\frac{q^n - q}{q + 1}$. Then the reduction modulo ℓ of a representation of degree $\frac{q^n + 1}{q + 1}$ either remains irreducible or it has two composition factors, one of them 1-dimensional, the other one equivalent to $\psi \pmod{\ell}$ tensored by a 1-dimensional one. Next, suppose that n is even. Then an ordinary Weil representation of degree $\frac{q^n + q}{q + 1}$ is reducible modulo any prime ℓ dividing $q + 1$; its reduction modulo ℓ has two irreducible constituents, one of dimension 1, the other one of dimension $\frac{q^n - 1}{q + 1}$. In fact, it is known that every ℓ -modular irreducible Weil representation lifts to characteristic 0. (This follows from results in [12, 23], but it is not stated there explicitly. For n even, see the last paragraph of the proof of [12, Theorem 7.2]; for n odd, see the proof of [23, Proposition 9].)

In the case where $G = GL(n, q)$, as noticed above, a generic Weil representation coincides with the permutation F -representation of G associated with the action of G on the vectors of the natural G -module, up to tensoring with a one-dimensional representation. It follows that the dimensions of the irreducible constituents of a generic Weil representation of $GL(n, q)$ are the same as those of the permutation representation in question. These are known to be $\frac{q^n - 1}{q - 1}$, $\frac{q^n - 1}{q - 1} - 1$, $\frac{q^n - 1}{q - 1} - 2$ or 1; for details see for instance [19, Theorem 9.1.4].

Finally, in the following Lemma we state a crucial property of Weil representations, concerning their restrictions to 'standard' subgroups:

Lemma 5.1. *Let $G \in \{GL(n, q), U(n, q), n > 2, Sp(2n, q), n > 1 \text{ and } q \text{ odd}\}$ and let V be the natural module for G . Let $V = W \oplus W'$ be a decomposition of V as a direct sum of subspaces, where W is non-degenerate if $G \neq GL(n, q)$, and set $S = \{g \in G \mid gW = W \text{ and } gw' = w' \text{ for all } w' \in W'\}$. Let ω be a generic, respectively irreducible Weil F -representation of G . Then $\omega|_S$ is a direct sum of generic, respectively irreducible Weil F -representations of S .*

Proof. The statement follows for arbitrary ℓ (coprime to q) if it holds for $\ell = 0$, by the very definition of ℓ -modular Weil representations. So let $\ell = 0$. It is known that the restriction of ω to S is the sum of generic Weil representations of S . (The proof is available in [52], and can be easily deduced from properties of extraspecial r -groups and their representations. See also [45, Proposition 2.2].) This immediately implies the claim for irreducible Weil representations.

At this point, it is worth to recall that every abelian subgroup A of a finite classical group G consisting of semisimple elements and orthogonally indecomposable, is cyclic. If A is irreducible and of maximal order, then A is called a Singer subgroup and its generators are called Singer cycles. If n is even, $U(n, q)$ and $SU(n, q)$ do not have Singer cycles. Likewise, $O^+(2n, q)$ and $O(2n + 1, q)$ do not have Singer cycles. If $G \in \{GL(n, q); SL(n, q); U(n, q), n \text{ odd}; SU(n, q), n \text{ odd}; Sp(2n, q); O^-(2n, q)\}$, then the order of a Singer cycle is known to be $q^n - 1$, $(q^n - 1)/(q - 1)$, $q^n + 1$, $(q^n + 1)/(q + 1)$, $q^n + 1$, $q^n + 1$, respectively.

Now, suppose that A is reducible. Clearly, by Maschke's theorem, such an A cannot occur in the groups $GL(n, q)$ and $SL(n, q)$. So we assume that G is not one of these two groups. It is well known (for details, see [27]) that V is a direct sum of two maximal totally singular A -stable subspaces V_1, V_2 of equal dimension. So V is of even dimension and of Witt index $\dim V/2$ in the case of unitary and orthogonal groups. Furthermore, A acts irreducibly on both V_1 and V_2 , and the actions of A on these subspaces are dual to each other. In particular, if $G \in \{Sp(2n, q), O^+(2n, q), U(n, q), n \text{ even}\}$, then $|A|$ divides $q^n - 1$. Moreover, if A is reducible and of maximal order, any generator of A will be called a Singer-type cycle of G .

An additional, simple but useful observation is that if an element $g \in G$ is semisimple and orthogonally indecomposable, then it is a power of a Singer cycle or of a Singer-type cycle. (This is a well known fact. For detailed arguments see [13, Lemmas 7.1 and 8.1].)

5.2. Orthogonally indecomposable elements. In this subsection we deal with the case when g is a semisimple and orthogonally indecomposable element of G .

As always, let F be an algebraically closed field of characteristic $\ell \neq r$. Recall that 1_G denotes the trivial FG -module, and ρ_G^{reg} the regular FG -module.

We first consider the generic Weil representations of G .

Lemma 5.2. (1) *Let $G = Sp(2n, q)$, where $n > 1$ and q is odd, or $G = U(n, q)$, where $n > 1$ is odd. Let $S = \langle g \rangle$, where g is a Singer cycle in G , and let ϕ be a generic Weil F -representation of G . Then $\phi(g)$ is a cyclic matrix.*

(2) *Let $G \in \{Sp(2n, q), \text{ where } n > 1 \text{ and } q \text{ is odd}; U(n, q), \text{ where } n > 2 \text{ is even}; GL(n, q), n > 2\}$, and let ϕ be a generic Weil F -representation of G . Let g be either a Singer cycle for $GL(n, q)$, or a Singer-type cycle for $G \neq GL(n, q)$ (in each case the order of g equals $q^n - 1$). Then $\phi(g)$ is an almost cyclic matrix and $\deg \phi(g) = |g|$.*

Proof. The cyclicity (respectively, almost cyclicity) of $\phi(g)$ in case (1) (respectively, case (2)) follows from the definition of a Weil representation and Lemma 3.2, items (1) and (2)(i), respectively. Lemma 3.2(2)(i) also implies the claim on $\deg \phi(g)$ in (2). We only have to observe that if $g \in U(n, q)$ is orthogonally indecomposable (resp., $g \in GL(n, q)$ is irreducible), then g is orthogonally indecomposable in its action on $E/Z(E)$ when it is viewed as a symplectic space. (Recall that the natural module for $G = U(n, q)$ can be embedded into a symplectic space of dimension $2n$ over F_q , preserving orthogonality. This is well known (e.g. see [30, 4.3, p.117]). In the case of $G = GL(n, q)$, the natural module can be embedded into $E/Z(E)$ as a maximal totally isotropic subspace.

Corollary 5.3. *Suppose that $h \in \langle g \rangle$, where g is as in (1) or (2) of Lemma 5.2, and $g \in \langle h, Z(G) \rangle$. Let τ be an irreducible Weil representation of G , with $\dim \tau > 1$. Then $\tau(h)$ is almost cyclic. Furthermore, $\deg \tau(g) = \deg \tau(h) = \min \{|g|/|Z(G)|, \dim \tau\}$. In particular, $\deg \tau(g) \geq \frac{|g|}{|Z(G)|} - 1$.*

Proof. Let M be the FG -module afforded by a generic Weil representation ϕ . It follows from Lemma 5.2, (1) and (2), that g yields an almost cyclic matrix in its action on every composition factor M' of M . Set $Z(G) = \langle z \rangle$. As $Z(G)$ acts scalarly on M' , the matrix of gz^i on M' is almost cyclic too. As $g = z^j h^k$ for some j, k , the matrix of h^k on M' is almost cyclic. This implies a similar claim for h . Whence the first statement of the Corollary.

For the second one, let M' be the module affording τ . If item (1) of Lemma 5.2 holds, then g is cyclic on M , and hence g is cyclic on M' . So $\deg \tau(g) = \dim M'$. A case-by-case inspection (as $|g|/|Z(G)| = (q^n + 1)/|Z(G)|$ and $\dim \tau$ are known), shows that $|g|/|Z(G)| \geq \dim \tau$, whence the result.

Next, suppose that item (2) of Lemma 5.2 holds.

If $G = GL(n, q)$, there is a one-dimensional FG -module L_1 , say, such that $M \otimes L_1$ is isomorphic to the permutation G -module L associated with the G -action on the vectors of the natural $F_q G$ -module V (see comments at the end of Section 5.1). So it suffices to assume that $M = L$. Let N be the submodule generated by the zero vector in V , so that M/N is isomorphic to the permutation G -module associated with the G -action on the non-zero vectors of V . It is obvious that the matrix of g on the latter module is cyclic, whence the claim (no matter what are dimensions of the irreducible constituents of M/N).

Next, we assume that G is unitary or symplectic. Then $|g| = q^n - 1$ and g is almost cyclic on M (but not cyclic). By Lemma 3.2(2), there exists a one-dimensional g -submodule N of M such that the matrix of g on M/N is cyclic. It then follows that there is at most one G -composition factor of M on which g is not cyclic. (This is true for an arbitrary G -module M admitting a one-dimensional G -submodule N such that g is cyclic on M/N . For, let M_1 be a proper G -submodule of M . If $N \subseteq M_1$, then M/M_1 is cyclic, and so are all composition factors of M/M_1 . As M_1/N is cyclic, the claim follows by induction on $\dim M$. If $N \cap M_1 = 0$ then M_1 is isomorphic to a submodule of M/N , and hence M_1 is cyclic. So again the claim follows by induction.)

Note that the dimensions of the composition factors belong to the set $\{1, |g|/|Z(G)|, (|g|/|Z(G)|) + 1\}$. If $\dim \tau = (|g|/|Z(G)|) + 1$, then $\tau(g)$ is not cyclic, but by the above $\deg \tau(g) = \dim \tau - 1$, and hence $\deg \tau(g) = |g|/|Z(G)|$, as claimed. If M has a composition factor of degree $(|g|/|Z(G)|) + 1$, then it is unique, and hence all the other non-trivial factors are cyclic g -modules of degree $|g|/|Z(G)|$. So if τ affords one of these factors then $\deg \tau(g) = \dim \tau$, and the second claim of the lemma follows in this case.

Finally, suppose that M has no composition factor of degree $|g|/|Z(G)| + 1$. This is not the case for $\ell = 0$. So suppose $\ell > 0$. Then after realizing the generic Weil representation by matrices over the ℓ -adic field integers, the module A , say, afforded by this representation, has a submodule series $0 = A_0 \subset A_1 \subset \cdots \subset A_d$, where $d = |Z(G)|$ and the quotients A_{i+1}/A_i correspond to the irreducible Weil representations. Therefore, $B := A \pmod{\ell}$ has a submodule series $0 = B_0 \subset B_1 \subset \cdots \subset B_d$, where B_{i+1}/B_i is the reduction of A_{i+1}/A_i modulo ℓ . Note that A is a Weil module in zero characteristic. So, as mentioned above, exactly one factor A_{i+1}/A_i has dimension $(|g|/|Z(G)|) + 1$, whereas the others are of dimension $|g|/|Z(G)|$. This is also true for the factors B_{i+1}/B_i . The factors A_{i+1}/A_i of dimension $|g|/|Z(G)|$ remain irreducible modulo ℓ , and the (single) one of dimension $(|g|/|Z(G)|) + 1$ is reducible modulo ℓ . Denote it by D , say. Clearly, the matrix of g on D is not cyclic. The above reasoning ensures that the matrix of g on every factor B_{i+1}/B_i other than D is cyclic. So we have to show that the matrix of g on the non-trivial composition factor D' , say, of D is cyclic. However, it is known that D' lifts to characteristic 0, so D' is isomorphic to a Weil representation obtained by reduction modulo ℓ of an irreducible representation of degree $|g|/|Z(G)|$. So the result follows.

Our next aim is prove the converse of Corollary 5.3, by showing that, if g is as in Lemma 5.2, the condition $g \in \langle Z(G), h \rangle$ is also necessary for $\tau(h)$ to be almost cyclic. We shall do this below (see Lemmas 5.5 and 5.7).

As the irreducible constituents of $\phi(G)$ remain irreducible under restriction to G' (provided $n > 2$ in the cases of $GL(n, q)$ and $U(n, q)$, and $(n, q) \neq (2, 2), (2, 3)$ if $G = Sp(2n, q)$), then this will imply the corresponding results for $SL(n, q)$ and $SU(n, q)$.

In order to make the proof of the subsequent lemma more transparent we explicitly state the following:

Lemma 5.4. (1) *Let S be a finite group and let Z a cyclic central subgroup of S . Set $Z = X \times Y$, where $X = \langle x \rangle$ is the Sylow ℓ -subgroup of Z . Then $\rho_S^{reg} = \bigoplus_{\lambda \in \text{Irr } Y} \lambda^S$, and for any fixed λ the quotient FS -modules $(1-x)^i \lambda^S / (1-x)^{i+1} \lambda^S$ for $i < |X|$ are isomorphic to each other and have dimension $|S : Z|$. In addition, the above quotients can be identified with the induced modules $\bar{\lambda}^S$, where $\bar{\lambda} \in \text{Irr } Z$, $\bar{\lambda}(X) = 1$ and $\bar{\lambda}(Y) = \lambda$.*

(2) *Let S be cyclic, $h \in S \setminus Z$ and $S_0 = \langle Z, h \rangle$. Then the matrix of h on $\bar{\lambda}^S$ is almost cyclic if and only if $S = S_0$. More precisely, if f_c is the characteristic polynomial of h on $\bar{\lambda}^S$ and f_m is the minimum polynomial, then $f_c = f_m^d$, where $d = |S : S_0|$.*

Proof. (1) By elementary properties of induced modules, as $X \cap Y = 1$, the module $\lambda^S|_X$ is the direct sum of $|S : Z|$ copies of ρ_X^{reg} . The Jordan form of x on λ^S shows that the quotient module $\lambda^S / (1-x)\lambda^S$ has dimension $|S : Z|$. Clearly, this holds for any subsequent factor $(1-x)^i \lambda^S / (1-x)^{i+1} \lambda^S$. On the other hand, the map which sends $v \in \lambda^S$ to $(1-x)v \in (1-x)\lambda^S$ induces an epimorphism of FS -modules from $\lambda^S / (1-x)\lambda^S$ to $(1-x)^i \lambda^S / (1-x)^{i+1} \lambda^S$. By dimension reasons, this is an isomorphism. The additional claim can be verified directly.

(2) Set $d = |S : S_0|$. Consider the restriction of $\bar{\lambda}^S$ to S_0 . We claim that this restriction is the direct sum of d copies of $\bar{\lambda}^{S_0}$. Set $A = Z(G)$, $B = S_0$. By the general theory of induced modules, $(\bar{\lambda}|_A)^S|_B$ is the direct sum of c copies of the modules $(\bar{\lambda}|_{A \cap B})^B$ (as S is abelian), where c is the number of the double cosets $A \setminus S / B$. In our case $c = |S|/|AB| = d$. Therefore, the matrix of h on $\bar{\lambda}^S$ is cyclic if $d = 1$ (as $\bar{\lambda}^S$ is a subquotient of $(1^{Z(G)})^S$),

otherwise this matrix is not even almost cyclic. In particular, this argument also proves the last claim.

Lemma 5.5. *Let $G \in \{Sp(2n, q), \text{ where } n > 1 \text{ and } q \text{ is odd}; U(n, q), n > 2, (n, q) \neq (3, 2); GL(n, q), n > 2\}$. Let g be as in Lemma 5.2(1), (2); so in particular g is of order $q^n \pm 1$. Let τ be an irreducible Weil F -representation of G , with $\dim \tau > 1$. Suppose that $h \notin Z(G)$ and $h \in \langle g \rangle$. Then the matrix $\tau(h)$ is almost cyclic only if $g \in \langle h, Z(G) \rangle$.*

Proof. Set $S = \langle g \rangle$, $\varepsilon = \pm 1$ and $|g| = q^n - \varepsilon$. Let M be the FG -module afforded by a generic Weil F -representation of G . By Lemma 3.2 (in view of the construction of the Weil representations), if $\varepsilon = -1$ then $M|_S$ is isomorphic to a submodule of codimension 1 in ρ_S^{reg} , the regular FS -module; whereas, if $\varepsilon = 1$ then ρ_S^{reg} is a submodule of codimension 1 in $M|_S$. Observe that $Z(G) \subset S$, and set $S_0 = \langle h, Z(G) \rangle$. We want to prove that, if $d := |S : S_0| > 1$, then the matrix $\tau(h)$ is not almost cyclic.

So, assume $d > 1$. Note that, for $G = U(n, q)$, this implies $(n, q) \neq (3, 2)$. Indeed, if $G = U(3, 2)$, then $\varepsilon = -1$ and $|g| = 9$. Thus $g^3 \in Z(G)$, and $d > 1$ forces $h \in \langle g^3 \rangle = Z(G)$.

We apply Lemma 5.4(2), choosing $Z = Z(G) = X \times Y$, where $X = \langle x \rangle$ is the Sylow ℓ -subgroup of Z , and $Y = \langle y \rangle$ (assuming $X = 1$ for $\ell = 0$). As $d > 1$, the matrix of h on $\bar{\lambda}^S$ is not almost cyclic. For each $\lambda \in \text{Irr } Y$ and for each $i < |X|$, set $N_\lambda^i = (1-x)^i \lambda^S / (1-x)^{i+1} \lambda^S$. Thus, N_λ^i affords the representation $\bar{\lambda}^S$ and $\dim N_\lambda^i = |S|/|Z|$ for every λ, i (see Lemma 5.4(1)).

According to Lemma 5.4(2), the action of h on N_λ^i can be represented by a block-diagonal matrix $\Delta = \text{diag}(D, \dots, D)$, where the number of the blocks is equal to $d = |S : S_0|$, and each block D is a cyclic matrix of size $|S_0 : Z|$. This implies that Δ is never almost cyclic. Moreover, denoting by R the underlying space N_λ^i of Δ , and assuming that R has a Δ -stable subspace R_1 of dimension at least $\dim R - 2$, we observe that $\Delta|_{R_1}$ is not almost cyclic, unless: either (i) $\dim R_1 = \dim R - 1$, $d = 2$ and $|S_0 : Z| = 2$; (ii) or $\dim R_1 = \dim R - 2$, $d = 2$ and $|S_0 : Z| \leq 3$. If case (i) holds, then $g^4 \in Z$. As $|g| = q^n \pm 1$ and $|Z| = 2, q+1, q-1$ for $G = Sp(2n, q), U(n, q), GL(n, q)$, respectively, we must have that $q^n \pm 1$ divides 8, $q^n \pm 1$ divides $4(q+1)$ and $q^n - 1$ divides $6(q-1)$, respectively. This implies $G = Sp(4, 3)$. For this group, the statement follows from Lemma 4.15. If case (ii) holds, then the above applies again if $|S_0 : Z| = 2$. If $|S_0 : Z| = 3$, then $g^6 \in Z$. Arguing as before, since for $G = Sp(2n, q), U(n, q), GL(n, q)$, respectively, we must have that $q^n \pm 1$ divides 12, $q^n - 1$ divides $6(q+1)$ and $q^n - 1$ divides $4(q-1)$, respectively. This could only hold for $G = U(3, 2)$, which is ruled out by our assumptions.

Now, for each $\lambda \in \text{Irr } Y$ set $M_\lambda = \{m \in M : ym = \lambda(y)m\}$. Observe that $M = \bigoplus_{\lambda \in \text{Irr } Y} M_\lambda$, where each M_λ is an FG -module, as $Y \subseteq Z(G)$. Moreover, every M_λ has a filtration $M_\lambda \supset (1-x)M_\lambda \supset (1-x)^2 M_\lambda \supset \dots$, again because $X \subseteq Z(G)$. Clearly, λ^S is the $\lambda(y)$ -eigenspace of y on ρ_S^{reg} , whereas M_λ is the $\lambda(y)$ -eigenspace of y on M . As mentioned above, $M|_S$ is isomorphic to a submodule of codimension 1 in ρ_S^{reg} if $\varepsilon = -1$, whereas, if $\varepsilon = 1$, ρ_S^{reg} is isomorphic to a submodule of codimension 1 in $M|_S$.

Set $M_\lambda^i := (1-x)^i M_\lambda / (1-x)^{i+1} M_\lambda$. Then the following holds: (i) if $\varepsilon = -1$, either $M_\lambda^i|_S \cong N_\lambda^i$ or $M_\lambda^i|_S$ is isomorphic to a submodule of codimension 1 in N_λ^i , so that $\dim M_\lambda^i \leq (|S|/|Z|)$; (ii) if $\varepsilon = 1$, either $M_\lambda^i|_S \cong N_\lambda^i$ or N_λ^i is isomorphic to a submodule of codimension 1 in $M_\lambda^i|_S$, so that $\dim M_\lambda^i \leq (|S|/|Z|) + 1$. This gives us information on $\dim M_\lambda^i$.

Let T be the FG -module afforded by τ . Clearly, we may identify T with a composition factor of M_λ^i for some i, λ , which we fix for the rest of our reasoning. The core of our argument is to show that either the FG -module M_λ^i is irreducible, or M_λ^i contains a composition factor of codimension 1, unless $G = GL(n, q)$, in which case the codimension may be 2. As a consequence, either T is isomorphic to M_λ^i , or has codimension 1 in M_λ^i , or $G = GL(n, q)$ and T has codimension 2 in M_λ^i . This, in view of the above formula $\text{diag}(D, \dots, D)$ for the matrix of h on N_λ^i , will prove that $\tau(h)$ is not almost cyclic, unless possibly when $G = GL(n, q)$ and M_λ^i contains no composition factor of codimension ≤ 1 .

In the latter case we shall adjust the matter (see below). We finally observe that our strategy depends on the comparison between the dimension of M_λ^i and the dimensions of the irreducible constituents of the generic Weil representations of G in cross characteristic, which have been described at the beginning of this section.

To avoid confusion, we prefer to argue case-by-case.

(1) Suppose $G = Sp(2n, q)$, $n > 1$, q odd.

First, let $\varepsilon = 1$. Then $\dim N_\lambda^i = (q^n - 1)/2$, and $(q^n - 1)/2 \leq \dim T \leq \dim M_\lambda^i \leq \dim N_\lambda^i + 1 = (q^n + 1)/2$. Whence the claim.

Let $\varepsilon = -1$. Then either $N_\lambda^i \cong M_\lambda^i|_S$ or $M_\lambda^i|_S$ is isomorphic to a submodule of N_λ^i of codimension 1. In the latter case M_λ^i is irreducible, and $T = M_\lambda^i$. In the former case $(q^n - 1)/2 \leq \dim T \leq \dim M_\lambda^i \leq \dim N_\lambda^i = (q^n + 1)/2$, and the claim follows again.

(2) Suppose $G = U(n, q)$, $n > 2$, n even. Then $\dim T \geq (q^n - 1)/(q + 1)$ and $\dim N_\lambda^i = |S/Z| = (q^n - 1)/(q + 1)$ (as only the case $\varepsilon = 1$ occurs). Thus, either $M_\lambda^i|_S \cong N_\lambda^i$ and M_λ^i is irreducible, or $M_\lambda^i|_S$ contains a submodule of codimension 1 isomorphic to N_λ^i . In both cases $\dim T \geq \dim M_\lambda^i - 1$, and we are done.

(3) Suppose $G = U(n, q)$, where $n \geq 3$ is odd. Here $\dim T \geq (q^n - q)/(q + 1)$ and $\dim N_\lambda^i = (q^n + 1)/(q + 1)$ (as only the case $\varepsilon = -1$ occurs).

If $M_\lambda^i|_S \cong N_\lambda^i$, then either $\dim M_\lambda^i = |S/Z| = (q^n + 1)/(q + 1)$, and hence $\dim T \geq \dim M_\lambda^i - 1$. If $M_\lambda^i|_S < N_\lambda^i$ then $\dim M_\lambda^i \geq (q^n - q)/(q + 1)$, and hence $T = M_\lambda^i$.

(4) Suppose $G = GL(n, q)$, $n > 2$. So $\varepsilon = 1$ and $|S/Z| = (q^n - 1)/(q - 1)$.

Let V be the underlying space for $GL(n, q)$, and let Π be the permutation FG -module associated with the natural action of G on V . Recall that $M = \Pi \otimes L$, where L is some one-dimensional FG -module. Therefore, τ is obtained from a constituent of Π by tensoring with a one-dimensional representation. Such tensoring does not affect almost cyclicity, so we may assume that $M = \Pi$. Let P_0 be the stabilizer in G of a non-zero vector of V , and let P the stabilizer of the line spanned by this vector. Then the representation afforded by Π is $1_G \oplus 1_{P_0}^G$. Therefore τ is a constituent of $1_{P_0}^G$, as $\dim \tau \neq 1$. For a moment, denote by M' the submodule of M afforded by $1_{P_0}^G$. As $\Pi = 1_G \oplus M'$, we can deal with M' in place of M . However, to simplify notation, we better rename as M the module afforded by $1_{P_0}^G$. As $S \cap P_0 = 1$ and now $\dim M = |S|$, we have $M|_S \cong \rho_S^{reg}$. This implies that $M_\lambda^i|_S \cong N_\lambda^i$. So $\dim M_\lambda^i = \dim N_\lambda^i = |S/Z| = (q^n - 1)/(q - 1)$.

As $P = P_0 \cdot Z(G)$, every one-dimensional representation λ of $Z(G)$ can be identified with a one-dimensional representation of P trivial on P_0 . By the so-called 'Subgroup Theorem' for induced modules, $\lambda^S = \lambda^G|_S$, as $G = SP$ and $S \cap P = Z(G)$. Furthermore, by the same theorem, $\lambda^G|_{G'} = \mu^{G'}$, where $\mu = \lambda|_{P \cap G'}$. By [19, Theorem 9.1.4], the dimension of any non one-dimensional irreducible constituent of $\mu^{G'}$ is at least $((q^n - 1)/(q - 1)) - e$, where $e = 1$ if ℓ does not divide $(q^n - q)/(q - 1)$, and $e = 2$ otherwise. Therefore, $\dim T \geq \frac{q^n - 1}{q - 1} - 2$.

It follows that $\dim M_\lambda^i \leq \dim T + 2$, as claimed.

We conclude that, in all the cases examined, the matrix of $\tau(h)$ is not almost cyclic.

Remark. Recall that every irreducible Weil F -representation of $GL(n, q)$, $n > 2$, (respectively, $U(n, q)$, $n > 2$) remains irreducible under restriction to $SL(n, q)$ (respectively, $SU(n, q)$). (This follows by degree reasons from the lower bounds known for non-trivial irreducible representations of $SU(n, q)$ and $SL(n, q)$, using Clifford's theorem.) Therefore, Lemma 5.5 applies to the case $h \in SL(n, q)$, $n > 2$, (respectively, $h \in SU(n, q)$, $n > 2$). Moreover, this allows us to limit ourselves to consider, with no loss of generality, the groups $GL(n, q), U(n, q)$ instead of all the groups G such that $SL(n, q) \subseteq G \subseteq GL(n, q), SU(n, q) \subseteq G \subseteq U(n, q)$ in Lemmas 5.8, 5.9 and 5.11 below.

Next, we examine in detail when the condition $g \in \langle h, Z(G) \rangle$ holds, under the assumption that h is a p -element. We distinguish two cases: (i) the case when $|h| = |g|$; (ii) the case when $|h| < |g|$.

The case when $|h| = |g|$ is dealt with by the following:

Lemma 5.6. (1) Let $G = Sp(2n, q)$, where $n > 1$ and q is odd, or $G = U(n, q)$, where $n > 1$ is odd. Let $g \in G$ be a Singer cycle for G . Suppose that $h \in \langle g \rangle$ and $|h| = |g|$ is a p -power. Then $G = U(3, 2)$ and $|g| = 9$.

(2) Let $G \in \{GL(n, q), n > 2; U(n, q), n > 2; Sp(2n, q), n > 1, q \text{ odd}\}$ and let $g \in G$ be either a Singer cycle for $GL(n, q)$ or a Singer-type cycle for $G \neq GL(n, q)$. Suppose that $h \in \langle g \rangle$ and $|h| = |g|$ is a p -power. Then one of the following holds:

(a) $G = Sp(4, 3)$ and $|g| = 8$;

(b) $G = SL(n, 2)$, n is an odd prime and $|g|$ is a Mersenne prime.

Proof. Suppose that $|g|$ is a prime-power and (1) holds. Then, by Lemma 2.6, one of the following holds: (i) $p = 2$ and $n = 1$ (which contradicts our assumptions), (ii) q is even and $q^n + 1 = p$ is a Fermat prime; (iii) $q^n + 1 = 9$, that is, $q^n = 8$. If (ii) holds then G is not symplectic, as q is even. As $q^n + 1$ is a prime, n is even. So G is not a unitary group. Finally, if (iii) holds, then $|g| = 9$, and $q^n = 8$, that is, $G = U(3, 2)$.

Next, suppose that $|g|$ is a prime-power and (2) holds. Then, by Lemma 2.6, either q is even and $|g| = q^n - 1$ is an odd prime, or $|g| = q^n - 1 = 8$, that is, $q^n = 9$. In the latter case $G = Sp(4, 3)$, in the former case $G = SL(n, 2)$ and n is a Mersenne prime.

Recall that a prime p is called a Zsigmondy prime for $q^n - 1$ if n is the least integer $i > 0$ such that p divides $q^i - 1$. This can be expressed by saying that n is the order of p modulo q . The classical Zsigmondy's theorem ([60]) states that a Zsigmondy prime for $q^n - 1$ exists for all pairs of integers n, q such that $n > 2$, $q > 1$ and $(n, q) \neq (6, 2)$.

The case when $|h| < |g|$ is dealt with by the following:

Lemma 5.7. Let $G \in \{GL(n, q), n > 2; U(n, q), n > 2, (n, q) \neq (3, 2); Sp(2n, q), n > 1, q \text{ odd}\}$ and let $g \in G$ be either a Singer or a Singer-type cycle for G . Furthermore, suppose that $g \in \langle h, Z(G) \rangle$, where $|h|$ is a p -power, $|h| < |g|$ and $h \in \langle g \rangle$. Then $p > 2$, $(p, |Z(G)|) = 1$, $\langle h \rangle$ is a Sylow p -subgroup of G , and one of the following holds:

(1) $G = GL(n, q)$, $|h| = (q^n - 1)/(q - 1)$ and $n \neq p$ is an odd prime;

(2) $G = Sp(2n, q)$, $|h| = (q^n + 1)/2$ and n is a 2-power;

(3) $G = Sp(2n, 3)$, $|h| = (3^n - 1)/2$ and $n \neq p$ is an odd prime;

(4) $G = U(n, q)$, $|h| = (q^n + 1)/(q + 1)$ and $n \neq p$ is an odd prime;

(5) $G = U(4, 2)$ and $|h| = 5$.

Proof. Obviously, $h \notin Z(G)$. Under our assumptions, $|h| = p^k$ for some integer $k > 0$. Furthermore $|Z(G)| > 1$, as $|h| < |g|$.

We first show that $(p, |Z(G)|) = 1$. Suppose the contrary. Assume first that $G = Sp(2n, q)$. Then $p = 2$ and $q^n \pm 1$ is a 2-power, which implies $q = 3$ and $n = 2$, that is, $G = Sp(4, 3)$ and $|g| = 8$. But in this case $\langle h \rangle$ contains $Z(G)$, and hence $g \notin \langle h, Z(G) \rangle$, against our assumption. If $G = GL(n, q)$, $(n, q) \neq (6, 2)$, we can apply Zsigmondy's theorem to find a prime $s \neq p$ that divides $|g|$ and does not divide $|Z(G)|$ (recall that $n > 2$ in this case). This contradicts the assumption $g \in \langle h, Z(G) \rangle$. The case $(n, q) = (6, 2)$ is trivial as $Z(G) = 1$. If $G = U(n, q)$, n even, then $|g| = q^n - 1$, and again by Zsigmondy's theorem, there is a prime t , say, dividing $q^n - 1$ but not $q^2 - 1$ (unless $(q, n) = (2, 6)$, but in this case $g \notin \langle h, Z(G) \rangle$). As $t \neq p$, we get a contradiction. Finally, if $G = U(n, q)$, n odd, then $|g| = q^n + 1$. By Zsigmondy's theorem, there is a prime u , say, dividing $q^{2n} - 1$, but neither $q^n - 1$ nor $q^2 - 1$. Here again we reach a contradiction.

Thus, p is coprime to $|Z(G)|$. This implies that $|g| = |h| \cdot |Z(G)|$ (by our assumption) and that $p > 2$. The latter claim is obvious if q is even, otherwise it follows from the fact that $|Z(G)| \in \{2, q \pm 1\}$.

Now, suppose that $|g| = q^n - 1$. First, observe that $(n, q) \neq (6, 2)$. (Otherwise $|Z(G)| = 3$. But this implies that $|h|$ is not a prime-power, against our assumptions.) Also, p is

the only Zsigmondy prime for $q^n - 1$. For, suppose that $t \neq p$, say, is another Zsigmondy prime for $q^n - 1$. Then, as $|g| = |h| \cdot |Z(G)|$, t divides $|Z(G)|$, whence G is unitary and $t|(q^2 - 1)$. This in turn implies $n = 2$, which is a contradiction as for unitary groups we assume $n > 2$.

Next, we claim that either (5) holds, or n is an odd prime different from p . For, suppose that $n = \nu t$ for some integers t, ν , where $1 < \nu < n$. Then p does not divide $q^\nu - 1$, which in turn implies that $q^\nu - 1$ divides $|Z(G)|$. This occurs if and only if (5) holds. So, assuming (5) does not hold, n is prime. Furthermore, n must be odd. For, $n = 2$ implies that $G = Sp(4, q)$ and $4|(q^2 - 1)$. But then $q^2 - 1 = |g| = |h| \cdot |Z(G)| = p^k \cdot 2$, a contradiction as $p > 2$. So n is odd. Now, suppose that $n = p$. Then p is a Zsigmondy prime for $q^p - 1$. However, since the Galois group of F_{q^p} over F_q is of order p , all the Galois group orbits on $F_{q^p} \setminus F_q$ are of size p . So $q^p - q = q(q^{p-1} - 1)$ is divisible by p . As p is coprime to q , it follows that p divides $q^{p-1} - 1$, a contradiction.

Additionally, we observe that if $G = Sp(2n, q)$ then $q = 3$. Indeed, we have $|g| = q^n - 1 = |Z(G)| \cdot |h|$ and $|h| < |g|$, so $|g| = 2 \cdot |h| = p^k \cdot 2$. As p is a Zsigmondy prime for $q^n - 1$, $(p, q - 1) = 1$. This forces $q - 1 = 2$, so (3) holds.

In conclusion: if $|g| = q^n - 1$, then one of the cases (1), (3), (5) holds.

Next, let us consider the cases where $|g| = q^n + 1$. First, observe that p is the only Zsigmondy prime for $q^{2n} - 1$. For, suppose that $t \neq p$, say, is another Zsigmondy prime for $q^{2n} - 1$. Then, as $|g| = |h| \cdot |Z(G)|$, t divides $|Z(G)|$, whence $t|(q^2 - 1)$, which is impossible, as $n > 1$. (Notice that $(2n, q) \neq (6, 2)$, since otherwise $G = U(3, 2)$, which is excluded by our assumptions).

Suppose first that $G = U(n, q)$. Then $n > 2$ is odd, and $|g| = q^n + 1 = |h| \cdot (q + 1)$, where $|h| = p^k$ for some $k > 0$. We claim that n is a prime different from p . For, suppose that $n = \nu s$, where $1 < \nu < n$. By the above, p is the unique Zsigmondy prime for $q^{2n} - 1$. On the other hand, $q^n + 1 = (q^\nu)^s + 1 = (q^\nu + 1)c = p^k(q + 1)$, for some integer c . As $\nu > 1$ is odd, this implies that p must divide $q^\nu + 1$, a contradiction. Assume that $n = p$. As above, by elementary Galois theory we obtain p divides $q^{2p} - q^2 = q^2(q^{2p-2} - 1)$. As p is coprime to q and does not divide $q^{2p-2} - 1$, we get a contradiction. So we have case (4) of the statement.

Finally, suppose that $G = Sp(2n, q)$ and $|h| = (q^n + 1)/2$. Then it is easily seen that n must be a 2-power. Indeed, suppose the contrary. Let $n = s \cdot d$, say, where s is an odd prime. Then $q^n + 1 = (q^d)^s + 1 = (q^d + 1)(q^{d(s-1)} - q^{d(s-2)} + \dots + 1)$, where both the factors in the last expression are greater than 2. It follows that p must divide $q^d + 1$, and hence $q^{2d} - 1$. A contradiction, as p is a Zsigmondy prime for $q^{2n} - 1$. So n is a 2-power, and we get case (2) of the statement.

We are left to show that $\langle h \rangle$ is a Sylow p -subgroup of G . To this end, recall that p is a Zsigmondy prime for $q^n - 1$ if this is the order of g , and for $q^{2n} - 1$ if $|g| = q^n + 1$. Then the well-known formulas for the orders of classical groups (e.g. see [30], p.19) show that $|G|_p = |q^n - 1|_p$ in the first case, and $|G|_p = |q^n + 1|_p$ in the second case. It follows that, for each group G under exam, the subgroup $\langle g \rangle$ contains a Sylow p -subgroup of G (which is therefore cyclic). Furthermore, as $\langle g \rangle = \langle h \rangle \times Z(G)$ and $(p, |Z(G)|) = 1$, we have $|h|_p = |g|_p$, and hence the Sylow p -subgroup of G contained in $\langle g \rangle$ coincides with $\langle h \rangle$.

Remark. The previous Lemma is clearly false when $G = U(3, 2)$. This solvable group can be fully handled by direct computation, looking at the character table and the Brauer character tables of G . Note that $|G| = 2^3 \cdot 3^4$, and we only need to examine the behaviour of non-scalar elements of order 3 and elements of order 9 (these are Singer cycles of G). Let τ be any irreducible F -representation of G . The following holds:

i) Let $\ell = 0$. Then almost cyclicity for g semisimple of prime-power order occurs if and only if: $|g| = 3$, g belongs to any non-scalar class (in the GAP labelling: classes 3c,d,e,f,g,i), and $\dim \tau = 2, 3$ (that is, τ is Weil); $|g| = 9$, g belongs to the classes 9a,9b (GAP labelling), and again $\dim \tau = 2, 3$. Here g is in fact cyclic.

ii) Let $\ell = 2$. The 2-modular irreducible representations of G have degrees 1, 3, 8. $\tau(g)$ is almost cyclic if and only if $|g| = 3$ or 9 and $\dim \tau = 3$. If $|g| = 9$, $\tau(g)$ is cyclic.

iii) Let $\ell = 3$. There are just two 3-modular non-trivial irreducible representations, of degrees 2 and 3, namely the Weil representations. In both cases all the elements of G of 3-power order are obviously represented by almost cyclic matrices.

As for $G = SU(3, 2)$, a group of order $2^3 \cdot 3^3$ with Sylow 3-subgroups of exponent 3, the following holds. Let $g \in G$ be a non-scalar element of order 3. Then:

- i) if $\ell = 0$, then $\tau(g)$ is almost cyclic if and only if $\dim \tau = 2, 3$.
- ii) if $\ell = 2$, then G has no irreducible 2-modular representations of degree 2, and $\tau(g)$ is almost cyclic if and only if $\dim \tau = 3$.
- iii) if $\ell = 3$, then $\tau(g)$ is almost cyclic if and only if $\dim \tau = 2, 3$.

5.3. Orthogonally decomposable elements. In this subsection we deal with the case when $g \in G$ is orthogonally decomposable. We begin with an auxiliary Lemma:

Lemma 5.8. *Let $G = U(n, q)$, where $n > 2$ is even and $(n, q) \neq (4, 2)$, and let $g \in G$ be an element of p -power order for some prime p , stabilizing a subspace W of V of dimension $n - 1$ and acting on W irreducibly (so $(p, q) = 1$). Let τ be an irreducible Weil representation of G . Then $\tau(g)$ is not almost cyclic.*

Proof. Observe that W^\perp is g -stable, and hence (as $n > 2$) $V = W \oplus W^\perp$ (so W is non-degenerate). Thus, g belongs to a subgroup H which can be identified with $U(W) \times U(W^\perp)$ (where the latter group is cyclic of order $q + 1$), and hence g is orthogonally decomposable. Let $g = g_1 g_2$, where $g_1 \in U(W)$, $g_2 \in U(W^\perp)$. Clearly both g_1 and g_2 are of p -power order. Let τ_0 be an irreducible constituent of $\tau|_H$ of dimension greater than 1. Then $\tau_0(g) = \tau_1(g_1) \otimes \tau_2(g_2)$, where τ_1 is an irreducible Weil representation of $U(W)$ of dimension greater than 1, and τ_2 is a 1-dimensional representation of $U(W^\perp)$ (see for instance [45, Lemma 4.2]).

By way of contradiction, suppose that $\tau(g)$ is almost cyclic. Then $\tau_1(g_1)$ is almost cyclic (as τ_2 is 1-dimensional). Since g_1 acts irreducibly on W , g_1 belongs to a Singer subgroup of $U(W)$. By Lemmas 5.2 and 5.5, $\langle g_1, Z(U(W)) \rangle$ is of order $q^{n-1} + 1$. As $(n, q) \neq (4, 2)$, the option $(n - 1, q) = (3, 2)$ recorded in Lemma 5.6, (1) is ruled out, and therefore we may apply Lemma 5.7 (where $G = U(n - 1, q)$ and $h = g_1$). We find that case (4) of Lemma 5.7 must hold, and hence $|g_1| = \frac{q^{n-1} + 1}{q + 1}$, where $p \neq n - 1$ is an odd prime. In addition, $P := \langle g_1 \rangle$ is a Sylow p -subgroup of $U(W)$, p is coprime to $q + 1$. It follows that $g_2 = 1$, and hence $g = g_1$. Furthermore, $(p, q^n - 1) = 1$. (Indeed, as p divides $q^{n-1} + 1$, it does not divide $q^n - 1 = q(q^{n-1} + 1) - (q + 1)$, as $(p, q + 1) = 1$.) So, in fact P is a Sylow p -subgroup of G . Indeed, $|G| = q^a(q^n - 1) \cdot |U(W)|$ for some natural number a , and hence p does not divide the index $|G : U(W)|$.

Recall that $\dim \tau \in \{\frac{q^n - 1}{q + 1}, \frac{q(q^{n-1} + 1)}{q + 1}\}$. Hence, $\dim \tau > |g| + 1$, as $|g| = \frac{q^{n-1} + 1}{q + 1}$. If $\ell \neq p$, then we may assume $\ell = 0$, as the irreducible Weil representations of G lift to characteristic zero. Thus, we only need to consider the cases $\ell = 0$ and $\ell = p$. If $\dim \tau$ is divisible by $|g|$, then τ is of p -defect 0, and hence $\tau(\langle g \rangle)$ is a direct sum of regular $F\langle g \rangle$ -modules. As we are assuming that $\tau(g)$ is almost cyclic, this implies that $\dim \tau = |g|$. But this is not the case.

So, suppose that $\dim \tau$ is not divisible by $|g|$. Then $\dim \tau = \frac{q^n - 1}{q + 1}$. It follows that $\dim \tau + 1 = q \cdot |g|$.

If $\ell = 0$, then by [37, Lemma 7.4] (here τ is one of the x'_i in [37, Lemma 7.4]), $\tau(\langle g \rangle)$ contains $q - 1$ regular $F\langle g \rangle$ -modules, plus the quotient of the regular $F\langle g \rangle$ -module by a one-dimensional submodule. This gives a contradiction.

Next, suppose $\ell = p$. In order to use Lemma 2.13, we show that the group $N_G(P)/P$ is abelian.

Set $N := N_G(P)$, and let $C_G(P) = P \cdot C$, where C is a complement of P . It is easy to see that C is abelian (indeed, $C = Z(U(W)) \times U(W^\perp)$). As W^\perp is obviously the fixed-point subspace of P on V , it follows that W^\perp , and hence also W , are N -stable. Thus, $N \subseteq H = U(W) \times U(W^\perp)$. Then, obviously, $[N, C] = 1$ and hence $C \subset Z(N)$. Let T be a complement of P in N . Then $C \subseteq T$ and T acts on P with kernel C . Since P is a cyclic p -group, where $p > 2$, $\text{Aut } P$ is cyclic. It follows that T is abelian, as $[T, C] = 1$, and so is $N_G(P)/P$ (being a cyclic extension of a central subgroup).

As P is a Sylow p -subgroup of G and $p = \ell$, by Lemma 2.13 the restriction to P of the FG -module M associated to τ decomposes (using the notation of Lemma 2.13) as $M|_P = \frac{\dim M - \dim L}{|P|} \rho_P^{\text{reg}} \oplus L$, where $L|_P$ is indecomposable and $\dim L < |P|$ (since $N_G(P)/P$ is abelian). By the above, $\dim M = \dim \tau = q \cdot |P| - 1$. This implies $\dim L \equiv -1 \pmod{|P|}$, whence $\dim L > 1$. As $\tau(g)$ is almost cyclic, this in turn forces $M|_P = L|_P$, which is not the case.

The following lemmas will be used for induction purposes:

Lemma 5.9. *Let $G = U(n, q)$, $n > 2$, $(n, q) \neq (3, 2)$, and let $g \in G$ be a non-scalar semisimple element of prime-power order dividing $2(q \pm 1)$. Let τ be an irreducible Weil representation of G , with $\dim \tau > 1$. Then $\tau(g)$ is almost cyclic if and only if one of the following holds:*

- (1) $G = U(3, 3)$, $|g| = 8$, and either $\dim \tau = 6$, or $\ell \neq 2$ and $\dim \tau = 7$;
- (2) $G = U(4, 2)$, $|g| = 3$, and either $\dim \tau = 5$, or $\ell \neq 3$ and $\dim \tau = 6$.

In addition, $\tau(g)$ is cyclic if and only if $G = U(3, 3)$ and $\dim \tau = 6$.

Proof. Let $G_1 = \langle SU(n, q), g \rangle$. Clearly G_1 is a normal subgroup of G . Let τ_1 be an irreducible constituent of $\tau|_{G_1}$. Then, by Clifford's theorem, $\dim \tau_1 > 1$. Indeed, otherwise, $SU(n, q)$ would lie in $\ker \tau_1$, and hence in $\ker \tau$. As $U(n, q)/SU(n, q)$ is abelian, this would imply $\dim \tau = 1$, which is not the case.

So, $\dim \tau_1 > 1$. Suppose that $\tau(g)$ (and hence $\tau_1(g)$) is almost cyclic. Let M_1 be the module afforded by τ_1 and suppose that neither $(n, q) = (3, 3)$, nor $n = 4$ and $|g|$ is a 2-power. Then, by Propositions 2.9 and 2.10, n suitable $SU(n, q)$ -conjugates of g suffice to generate G_1 . Thus, by Lemma 2.11, $\dim M_1 \leq n \cdot (|g| - 1) \leq n \cdot (2q + 1)$. As $\dim M_1 \geq (q^n - q)/(q + 1)$ (see [31]; the exceptions for $SU(4, 2)$, $SU(4, 3)$ recorded in [31] occur only for projective representations), it follows that $n \cdot (2q + 1) \geq (q^n - q)/(q + 1)$, or equivalently $n(q + 1)(2q + 1) \geq q(q^{n-1} - 1)$. But this only holds if either $n = 3$ and $q \leq 7$, or $n = 4$ and $q \leq 3$, or $n = 5, 6$ and $q = 2$.

Direct computations using the GAP package show that, if $n = 3$ and $4 \leq q \leq 7$, $\tau(g)$ is not almost cyclic, whereas if $(n, q) = (3, 3)$ the exceptional case listed in (1) arises.

If $n = 4$ and $|g|$ is not a 2-power, then, by the above, only the case $G = U(4, 2)$ needs to be examined. This case is dealt with by Lemma 4.16, yielding the exceptional item listed in (2).

So, suppose that $n = 4$ and $|g|$ is a 2-power. Then, by Proposition 2.10(2), as g is semisimple, four suitable $SU(4, q)$ -conjugates of g suffice to generate G_1 . In this case, the condition $(q^4 - q)/(q + 1) \leq \dim M_1 \leq 4 \cdot (2q + 1)$ must hold, and this only happens if $q \leq 3$. Computations using GAP rule out the case $q = 3$. The case $q = 2$ may be ignored, as g is semisimple.

Finally, suppose that $n = 5, 6$ and $q = 2$. The case $n = 6$ is easily ruled out, since on one hand $\dim M_1 \leq n(|g| - 1) = 12$, but on the other hand $(q^n - q)/(q + 1) \geq 20$. So, assume that $G = U(5, 2)$ and let V be the natural module for G . Since $|g| = 3$, g is diagonalizable on V , and hence has an eigenspace of dimension at least 2 on V , by dimension reasons. Therefore, g stabilizes an isotropic 1-dimensional subspace, say, W . Then $g \in P$, where P is the stabilizer of W in G . Let U be the unipotent radical of P . We know that g acts faithfully by conjugation on $U/Z(U)$. Set $X = \langle g, U \rangle$, and let ϕ be an irreducible constituent of $\tau|_X$, non-trivial on $Z(U)$. Set $E = \phi(U)$. Then E is a group of symplectic

type, and $E/Z(E) \cong U/Z(U)$ has order 2^6 (see [8]). However, as $\phi(g)$ is assumed to be almost cyclic, Lemma 3.7 implies that $|g| = 2^3 \pm 1$, a contradiction, as $|g| = 3$.

Lemma 5.10. *Let $G \in \{U(n, q), n > 2, Sp(2n, q), n > 1 \text{ and } q \text{ odd}\}$, and let $H = G_1 \times G_2$, where H is the stabilizer in G of a non-degenerate m -dimensional subspace W of the natural module for G (so $G_1 = C_H(W^\perp), G_2 = C_H(W)$). Suppose that G_1 is non-solvable. Let τ be an irreducible Weil F -representation of G . Then either $\tau|_H$ contains an irreducible constituent ϕ such that $\phi = \phi_1 \otimes \phi_2$, where ϕ_1, ϕ_2 are irreducible Weil F -representations of G_1, G_2 , both of dimension greater than 1, or one of the following holds:*

- (1) $G = U(n, q)$ and $n - m = 1$;
- (2) $G = Sp(2n, 3)$, $G_2 \cong Sp(2, 3)$ and $\ell = 2$; in this case the restriction of τ to the derived subgroup of H contains at least 2 isomorphic composition factors of dimension greater than 1;
- (3) $G = U(n, 2)$, $\ell = 3$ and $G_2 \cong U(2, 2)$; in this case the restriction of τ to the derived subgroup of H contains at least 2 isomorphic composition factors of dimension greater than 1.

Proof. Suppose that (1) does not hold.

Case (i): G_2 is non-solvable.

Suppose first that $\ell = 0$. Let ω be a generic Weil representation of G . Then the restriction of ω to G_i ($i = 1, 2$) is the sum of generic Weil representations of G_i by Lemma 5.1. It follows that $\omega|_H$ is the sum of irreducible representations of shape $\phi_1 \otimes \phi_2$, where ϕ_1, ϕ_2 are irreducible Weil representations of G_1, G_2 , respectively. Therefore, this is also true for $\tau|_H$. As we assume that G_1, G_2 are both non-solvable, neither of them has an irreducible Weil representation of dimension 1. So we are done in the case $\ell = 0$.

Now, suppose that $\ell > 0$. Recall that τ lifts to characteristic 0. Let $\bar{\tau}$ be the lift of τ , and let $\bar{\phi}$ be a composition factor of $\bar{\tau}|_H$. Then every composition factor of $\bar{\phi} \pmod{\ell}$ is a composition factor of $\tau|_H$. Let $\bar{\phi} = \bar{\phi}_1 \otimes \bar{\phi}_2$, where $\bar{\phi}_1, \bar{\phi}_2$ are irreducible representations of G_1, G_2 , respectively (both of dimension greater than 1). Then $\bar{\phi} \pmod{\ell}$ contains all the composition factors of $\bar{\phi}_1 \pmod{\ell} \otimes \bar{\phi}_2 \pmod{\ell}$. Clearly, each $\bar{\phi}_i \pmod{\ell}$ ($i = 1, 2$) contains a composition factor of dimension greater than 1, otherwise $\bar{\phi}_i \pmod{\ell}$ would be solvable. Setting $\phi = \bar{\phi} \pmod{\ell}$, the result follows.

Case (ii) G_2 is solvable.

Then either $G_2 \cong Sp(2, 3)$ or $G_2 \cong U(2, 2), U(2, 3), U(3, 2)$. In each case G_2 is non-abelian. Again, let us start with the case $\ell = 0$. As τ is faithful on G_2 , $\tau|_{G_2}$ has an irreducible constituent ϕ_2 , say, of dimension at least 2. It follows that $\tau|_H$ has an irreducible constituent $\phi = \phi_1 \otimes \phi_2$, where ϕ_1 is an irreducible Weil representation of G_1 , as required. Now, let $\ell > 0$, and let ϕ be chosen as above. If ℓ is coprime to the order of G_2 , that is, $\ell \notin \{2, 3\}$, $\phi \pmod{\ell}$ behaves like ϕ , and we are done. So we may assume that $\ell = 2$ if $q = 3$, and $\ell = 3$ if $q = 2$. If $G_2 \cong Sp(2, 3)$, then $G_2/O_2(G_2)$ is of order 3. So the reduction modulo 2 of the 2-dimensional Weil representation of G_2 is a completely reducible non-trivial representation of dimension 2. It follows that $\phi \pmod{2}$ is the direct sum of two representations of H , which are isomorphic under restriction to $H' = G_1 \times O_2(G_2)$. This gives us case (2) of the statement. If $G_2 \cong U(2, 2)$, then $G_2/O_3(G_2)$ has order 2, so the reduction mod 3 of the 2-dimensional Weil representation of G_2 is a completely reducible non-trivial representation of dimension 2. It follows that $\phi \pmod{3}$ is the direct sum of two representations of H , which are isomorphic under restriction to $H' = G_1 \times O_3(G_2)$. Finally, in both $U(2, 3)$ and $U(3, 2)$, the reduction mod ℓ of an ordinary irreducible Weil representation contains a composition factor of dimension greater than 1. This gives case (3) of the statement.

Lemma 5.11. *Suppose that $G = U(n, q)$, where $n > 2$ and $(n, q) \neq (5, 2), (4, 2), (3, 3), (3, 2)$. Let $g \in G$ be a non-scalar semisimple element of p -power order for some prime p , and*

let τ be an irreducible Weil F -representation of G . Suppose that $\tau(g)$ is almost cyclic. Then $n \neq p$ is an odd prime, g is irreducible of order $(q^n + 1)/(q + 1)$, and $\langle g \rangle$ is a Sylow p -subgroup of G .

Proof. Suppose that $g \in G$ is orthogonally indecomposable. Then (taking into account Lemma 5.6) our g satisfies the assumptions on h in Lemma 5.7, and therefore the result follows from that lemma.

So, assume that g is orthogonally decomposable. We aim to show that this cannot occur.

Let V be the natural module for G , let W be a non-degenerate g -stable subspace of V such that $g|_W$ is orthogonally indecomposable, and choose W such that $|g| = |g|_W|$. Set $m = \dim W$. By Lemma 5.9, we can assume that $m > 2$. (Indeed, otherwise, $|g|$ divides $q^2 - 1$; as $|g|$ is a prime power, $|g|$ divides either $2(q + 1)$ or $2(q - 1)$. This is impossible by Lemma 5.9, as we exclude the cases $(n, q) = (4, 2), (3, 3)$.)

So $m > 2$, and g belongs to a subgroup $H = G_1 \times G_2$, where $G_1 \cong U(m, q)$ and $G_2 \cong U(n - m, q)$. Let $g = g_1 g_2$, where $g_1 \in G_1$, $g_2 \in G_2$. Then $|g| = |g_1|$; moreover, either m is odd and $|g|$ divides $q^m + 1$, or m is even and $|g|$ divides $q^m - 1$.

We first rule out the second possibility. Indeed, let $|g|$ divide $q^m - 1$ and set $G_3 = \langle G_1, g \rangle = \langle G_1, g_2 \rangle$. Then $G_3 = G_1 \cdot Z(G_3)$. Let ϕ be an irreducible constituent of $\tau|_{G_3}$ of dimension greater than 1. By Schur's lemma, $\phi(g)$ is a scalar multiple of $\phi(g_1)$. As $\phi|_{G_1}$ is a Weil representation of G_1 by Lemma 5.1, then, by Lemmas 5.6 and 5.7, $G_1 \cong U(4, 2)$ and $|g_1| = 5$. In this case $\dim \phi = 5$ or 6 . By Corollary 5.3, $\deg \phi(g_1) = 5$. If $g_2 = \text{Id}$, then $G_3 = G_1$ is contained in a subgroup $H_1 = SU(5, 2)$ (the pointwise stabilizer of a non-degenerate subspace of W^\perp of dimension $n - 5$). So, we may assume that $g \in H_1$. Suppose first that $\ell = 5$. As a Sylow 5-subgroup S of H_1 is cyclic and $N_{H_1}(S)$ is abelian, it follows from Lemma 2.13 and Corollary 2.14 that every irreducible constituent of $\tau|_{H_1}$ is of degree at most 6. However, inspection of the Brauer character tables for all $\ell \neq 2$ in [29] shows that the minimum dimension of a non-trivial irreducible F -representation of H_1 is 10, a contradiction. Next, suppose that $\ell \neq 5$. By Proposition 2.9, H_1 can be generated by five conjugates of g_1 , and hence, by Lemma 2.11, we only need to examine F -representations of $SU(5, 2)$ of degree at most 20. However, inspection of the character table and the Brauer character tables of H_1 shows that such representations can only have degree 10 or 11, with character or Brauer character having respectively value equal to 0 or 1 on elements of order 5. This obviously implies that $\tau(g)$ is not almost cyclic, a contradiction. So, suppose that $g_2 \neq \text{Id}$, and hence $|g_2| = 5$. Then $\dim W^\perp \geq 4$ (as $U(n - m, 2)$ does not have elements of order 5 for $n - m \leq 3$); in particular, both G_1 and G_2 are not solvable. By Lemma 5.10, we can choose τ so that $\tau|_H$ contains an irreducible constituent of shape $\tau_1 \otimes \tau_2$, where $\dim \tau_i > 1$. Then, by Lemmas 2.3 and 2.4, the matrix $\tau_1(g_1) \otimes \tau_2(g_2)$ is not almost cyclic, again a contradiction.

Thus, $|g|$ divides $q^m + 1$. Observe that $n - m > 1$. Otherwise $m = n - 1$, but this option is ruled out by Lemma 5.8 (note that g acts irreducibly on W). In fact, this lemma also rules out the case $n - m = 2$. Indeed, if $g_2 \in U(2, q)$, then $|g_2|$ divides $2(q \pm 1)$ and $q^m + 1$. As m is odd, $\frac{q^m + 1}{q + 1}$ is odd, so $(q^m + 1, 2(q + 1)) = q + 1$, and either $(q^m + 1, 2(q - 1)) = 2$, or $4|(q + 1)$ and hence $(q^m + 1, 2(q - 1)) = 4$. In both cases $|g_2|$ divides $q + 1$. It follows that g_2 stabilizes a non-degenerate subspace of dimension 1 on W^\perp . In this case g belongs to a subgroup X , say, isomorphic to $X_1 \times X_2$, where $X_1 = U(n - 1, q)$, $X_2 = U(1, q)$, and the restriction $\tau|_X$ contains an irreducible constituent ϕ , say, non-trivial on the commutator subgroup of X_1 . Thus, we may apply Lemma 5.8 to ϕ , getting that $n - m > 2$, unless $G = U(5, 2)$. But this case is ruled out by our assumptions.

Now, suppose first that G_1 is not solvable. Then, by the above, $2 < m < n - 2$. Again by Lemma 5.10, the restriction of τ to $G_1 \times G_2$ contains a composition factor λ of shape $\lambda_1 \otimes \lambda_2$, where λ_i is an irreducible Weil representation of G_i and $\dim \lambda_i > 1$ for $i = 1, 2$.

Let $\ell \neq p$. Then the matrix $\lambda_1(g_1)$ is cyclic (see Lemma 2.2), and hence, by Lemmas 5.6 and 5.7 applied to $\lambda_1(g_1)$, case (4) of Lemma 5.7 holds for $\lambda_1(g_1)$. In particular, p is coprime to $q + 1$, whence, by Corollary 5.3, $\deg \lambda_1(g_1) \geq |g_1| - 1 = |g| - 1$.

Clearly, neither $\lambda_1(g_1)$ nor $\lambda_2(g_2)$ are scalar, otherwise the matrix of $\lambda(g)$ is not almost cyclic. In particular, $\deg \lambda_2(g_2) \geq 2$. Set $k = \deg \lambda_1(g_1)$, $l = \deg \lambda_2(g_2)$. Then $k \geq l$. (Indeed, otherwise $l = |g|$, as $k \geq |g| - 1$. By Lemma 2.2, $|g| \geq kl - \min\{k, l\} + 1 \geq (|g| - 1)|g| - (|g| - 1) + 1 = |g|^2 - 2|g| + 2$, whence $|g| \leq 2$, a contradiction.) So $\min\{k, l\} = l$, and hence, by Lemma 2.2, $|g| \geq kl - l + 1 = (k - 1)l + 1 \geq 2(|g| - 2) + 1$ (as $l \geq 2$), whence $|g| = 3$. Since $\lambda_1(g_1)$ is cyclic, it follows that $\dim \lambda_1 \leq 3$, which is not the case, as G_1 is not solvable.

So, let $\ell = p$. By Lemma 2.4, $\deg \lambda_1(g_1) \leq 2$. Since $\deg \lambda_1(g_1) \geq |g| - 1$, this implies $|g| \leq 3$. As above, this leads to a contradiction with the assumption $2 < m < n - 2$.

We are left with the case where G_1 is solvable. Thus $q = 2$, and $m = 3$. Suppose first that G_2 is also solvable. Then $n - m = 3$, and hence $G = U(6, 2)$ and $|g| = 9$, by Lemma 5.9. But this case is ruled out by Lemma 4.18. Next, suppose that G_2 is not solvable. Then $n \geq 7$. Furthermore, by Lemma 5.9, we may assume that $|g| = 9$. Let W' be a minimal non-zero non-degenerate g -stable subspace of V lying in W^\perp . It is easy to see that either $\dim W' = 1$ or $\dim W' = 3$. Indeed, suppose that $\dim W' = 2$. Then $g|_{W'}$ has order 3 and acts irreducibly on W' ; hence its minimum polynomial has degree 3 and splits over F_4 . But this implies that g is reducible on W' , a contradiction. Next, suppose that $\dim W' > 2$. Observe that g^3 is diagonalizable over F_4 , and hence acts scalarly on W' . This implies that $\dim W' < 4$, and we conclude that $\dim W' = 3$. Since $n \geq 7$, it follows that there exists a 6-dimensional non-degenerate g -stable subspace W_1 of V containing W . Set $Y_1 = U(W_1)$, $Y_2 = U(W_1^\perp)$, and let Y be the stabilizer of W_1 in G . Clearly $Y \cong Y_1 \times Y_2$. Let us write $g = y_1 y_2$, where $y_1 \in Y_1$ and $y_2 \in Y_2$. Note that $|y_1| = 9$. Let σ be an irreducible constituent of $\tau|_Y$ non-trivial on Y_1' . Then $\sigma = \sigma_1 \otimes \sigma_2$ and $\sigma(g) = \sigma_1(y_1) \otimes \sigma_2(y_2)$. As $\tau(g)$ is almost cyclic, so are $\sigma(g)$ and $\sigma_1(y_1)$. This contradicts Lemma 4.18.

Proposition 5.12. *Let $G = Sp(2n, q)$, where $n > 1$, q is odd and $G \neq Sp(4, 3)$. Let $g \in G$ be a non-scalar semisimple orthogonally decomposable element of p -power order, and let τ be an irreducible Weil F -representation of G of dimension greater than 1. Then $\tau(g)$ is not almost cyclic.*

Proof. (A) We first rule out the case where $q = 3$, $\ell = 2$ and V contains a g -stable 2-dimensional non-degenerate subspace X , say. In this case, g is contained in a subgroup $K = K_1 \times K_2$, where $K_1 = Sp(X)$ and $K_2 = Sp(X^\perp)$. In particular, K_2 is not solvable (otherwise $G = Sp(4, 3)$). Let $g = g_1 g_2$, where $g_1 \in K_1, g_2 \in K_2$. As g_1 is semisimple and K_1/K_1' is of order 3, we have $g_1 \in K_1$. As K_2 is perfect, $g \in K'$. By Lemma 5.10(2), $\tau|_{K'}$ contains at least two isomorphic composition factors of dimension greater than 1. Therefore, $\tau(g)$ is not almost cyclic, and the claim follows.

(B) Next, let us show that g has no 1- or -1 -eigenspace on V . Indeed, suppose the contrary. Observe that any such eigenspace is non-degenerate. So, clearly, in any of them we can choose a non-degenerate g -stable subspace X , say, of dimension 2. Thus, g is contained in a subgroup $H = G_1 \times G_2$, where $G_1 = Sp(X^\perp)$ and $G_2 = Sp(X)$. Suppose that G_1 is solvable. Then $G = Sp(4, 3)$, which is against our assumption. So we may assume that G_1 is not solvable. It follows, by Lemma 5.10, that there is an irreducible constituent ϕ of $\tau|_H$ such that $\phi = \phi_1 \otimes \phi_2$, where $\phi_1 \in \text{Irr } G_1$, $\phi_2 \in \text{Irr } G_2$ and either both ϕ_1, ϕ_2 are of dimension greater than 1, or $q = 3, \ell = 2$. The latter case is ruled out in (A). In the former case $\phi(g)$ is obviously not almost cyclic.

From now on, we choose W to be a non-degenerate g -stable subspace of V such that $g|_W$ is orthogonally indecomposable, and W is of maximal dimension with this property. Set $2m = \dim W$. So $g \in H = G_1 \times G_2$, where $G_1 \cong Sp(2m, q)$ and $G_2 \cong Sp(2n - 2m, q)$. Set $g = g_1 g_2$, where $g_1 \in G_1, g_2 \in G_2$.

(C) Suppose that G_1 is solvable. Then $G_1 = Sp(2, 3)$, and g stabilizes a direct sum of non-degenerate two-dimensional subspaces of V (by our choice of W). So $|g| \leq 4$. We can assume $\ell \neq 2$ by (A). If g^2 is not scalar, g must have a 1- or a -1 -eigenspace. But this case has been ruled out in (B). So we are left with the case where $g^2 = \pm \text{Id}$. As above, since $\ell \neq 2$, by Lemma 5.10 there is an irreducible constituent ϕ of $\tau|_H$ such that $\phi = \phi_1 \otimes \phi_2$, where $\phi_1 \in \text{Irr } G_1$, $\phi_2 \in \text{Irr } G_2$ and both ϕ_1, ϕ_2 are of dimension greater than 1. Therefore, $\phi_i(g_i)^2 = \pm \text{Id}$ for $i = 1, 2$. However, the tensor product of any two matrices over F of size greater than 1 whose squares are scalar cannot be almost cyclic (by Lemma 2.2).

In view of the above, from now on we may assume that G_1 is not solvable.

(D) Suppose that $G_2 \cong Sp(2n - 2m, q)$ is solvable. So $G_2 = Sp(2, 3)$. By (B), $g_2 \neq \text{Id}$, so $|g_2|$, and hence also $|g_1|$, is a non-trivial 2-power. Moreover, by our choice of W , g_1 is orthogonally indecomposable. By Lemma 5.10, there is an irreducible constituent ϕ of $\tau|_H$ such that $\phi = \phi_1 \otimes \phi_2$, and $\dim \phi_i > 1$ for $i = 1, 2$. Assume that $\tau(g)$ is almost cyclic. Then $\phi(g)$ is also almost cyclic, and therefore $\phi_i(g_i)$ is cyclic for $i = 1, 2$, in view of Lemma 2.2. As g_1 is orthogonally indecomposable, g_1 is either a power of a Singer cycle, or a power of a Singer-type cycle of $Sp(2r, 3)$. It follows from Lemmas 5.5 and 5.7 applied to $\phi_1(g_1)$, that g_1 itself is either a Singer cycle or a Singer-type cycle. By Lemma 2.6, either $m = 2$ and $|g_1| = 3^2 - 1 = 8$, or $m = 1$ and $G_1 = Sp(2, 3)$. The latter case is ruled out, as G_1 is non-solvable. In the former case $G = Sp(6, 3)$ and $G_1 = Sp(4, 3)$. By (A) applied to $Sp(6, 3)$, we can assume $\ell \neq 2$. As $g_1^4 \in Z(G_1)$, $\phi_1(g_1^4)$ is scalar. By Lemma 4.15, $\dim \phi_1(g_1) = 4$ (as $\phi_1(g_1)$ is cyclic) and the spectrum of $\phi_1(g_1)$ consists of four distinct 4-roots of -1 . Denote this set by S , say. In turn, as $G_2 \cong Sp(2, 3)$, we have $g_2^4 = 1$. Note that $S \cdot \alpha = S$ for every 4-root α of 1. Therefore, $\phi(g)$ consists of 4-roots of -1 , each of multiplicity equal to $\dim \phi_2$, a contradiction.

(E) Suppose that $|g|$ divides $q + 1$ or $q - 1$ (it is convenient to consider this case separately). By Propositions 2.9 and 2.10, G can be generated by at most $2n$ conjugates of g unless $n = 2$ and $g^2 \in Z(G)$, in which case G can be generated by at most 5 conjugates of g . Suppose that $\tau(g)$ is almost cyclic. In the exceptional case, it follows from Lemma 2.11 that $\dim \tau \leq 5$; as $\dim \tau \geq (q^2 - 1)/2$, this implies $q = 3$, which is ruled out by our assumptions. Otherwise, again by Lemma 2.11, $\dim \tau \leq 2n(|g| - 1) \leq 2nq$. As $\dim \tau \geq (q^n - 1)/2$, this implies $q^n \leq 1 + 4nq$, whence either $n = 2, q \leq 7$ or $n = 3, q = 3$.

Suppose that $n = 2, q \leq 7$. Then either $p = 2$ or $|g| = 3$. In the latter case, the above bound reduces to $\dim \tau \leq 8$, whence $q^2 \leq 17$. This implies $q = 3$, which contradicts our assumptions. Now, we are left with the cases $p = 2$ and $(n, q) \in \{(2, 5), (2, 7), (3, 3)\}$. Clearly, in view of (B), $|g| \neq 2$. Suppose that $|g| = 4$. As $g^2 \notin Z(G)$, $g^2 \neq -\text{Id}$, and hence g acts as an element of order 2 on the 1-eigenspace of g^2 . But this contradicts (B). Therefore, the case $(n, q) = (3, 3)$ is ruled out, and are left with the case $|g| = 8$, $G = Sp(4, 7)$.

Thus, $G_1 \cong G_2 \cong SL(2, 7)$. The restriction of τ to $H = G_1 \times G_2$ is easy to describe for $G = Sp(4, q)$ and $G_1 \cong G_2 \cong Sp(2, q)$ (e.g. see [51], Theorem 2). Namely. let λ_i, μ_i ($i = 1, 2$) be the irreducible Weil representations of G_i of degree $(q - 1)/2$ and $(q + 1)/2$, respectively, over the complex numbers. Then $\tau|_H = (\lambda_1 \otimes \mu_2) \oplus (\lambda_2 \otimes \mu_1)$ if $\dim \tau = (q^2 - 1)/2$, whereas $\tau|_H = (\lambda_1 \otimes \mu_1) \oplus (\lambda_2 \otimes \mu_2)$ if $\dim \tau = (q^2 + 1)/2$. Recall that the representations λ_i, μ_i remain irreducible modulo any $\ell \neq 2$, so these formulae are valid for any $\ell \neq 2$. Furthermore, as $q = 7$, we have $\dim \lambda_i = 3$ and $\dim \mu_i = 4$. On the other hand, the representations μ_i under reduction mod 2 contain a composition factor isomorphic to λ_i mod 2. Thus, by Lemma 2.4, we may assume that $\ell \neq 2$.

By Lemma 2.2, $\lambda_1(g_1) \otimes \mu_2(g_2)$ is cyclic if $\tau(g)$ is so. This implies $\deg \tau(g) \geq 12 - 3 + 1 = 10$, which is a contradiction, as $|g| = 8$. Similarly, we get a contradiction considering $\lambda_1(g_1) \otimes \mu_1(g_2)$. This completes the argument for $p = 2$.

(F) Finally, suppose that both G_1 and G_2 are not solvable. Then, again by Lemma 5.10, there is an irreducible constituent ϕ , say, of $\tau|_H$ such that $\phi = \phi_1 \otimes \phi_2$, where ϕ_1, ϕ_2

are irreducible Weil representations of G_1, G_2 , respectively, both of dimension at least 2. Thus, $\phi(g) = \phi_1(g_1) \otimes \phi_2(g_2)$. As in (D), assuming that $\tau(g)$, and hence $\phi(g)$, is almost cyclic, it follows from Lemma 2.2 that $\phi_1(g_1)$ and $\phi_2(g_2)$ are cyclic. In particular, g_1 and g_2 are not scalar.

(i) Assume first that $\ell = p$. By Lemma 2.4, $\phi(g)$ is not almost cyclic unless $\ell \neq 2$ and $\dim \phi_i = 2$ for $i = 1, 2$. As $\dim \phi_2 \geq (q^{n-m} - 1)/2$ and $n - m \geq 1$, the equality $\dim \phi_2 = 2$ implies $n - m = 1$ and $q = 3$ or 5 . As G_2 is not solvable, we are left to examine the case where $G_2 = Sp(2, 5)$. Similarly, $\dim \phi_1 = 2$ implies $G_1 = Sp(2, 5)$. In addition, $\ell = p = 3$, as $p = \ell \neq 2, 5$. Therefore, $G = Sp(4, 5)$ and $|g| = 3$. Note that, by Lemma 5.1, $\tau|_{G_i}$ is a sum of irreducible Weil representations of G_i . As $\ell = 3$, none of them is one-dimensional. (Indeed, the irreducible Weil representations of $Sp(2, 5)$ are of dimension 2 and 3 in characteristic 0. Both of them remain irreducible modulo 3, the former by dimension reasons, and the latter by the fact that it is of 3-defect 0.) So $\tau(g)$ is not almost cyclic, unless $\dim \tau = \dim \phi = 4$. However, $\dim \tau > 4$.

(ii) Now, assume that $\ell \neq p$. The case where $m = 1$ is ruled out by (E). Indeed, if $m = 1$, then every orthogonally indecomposable g -stable subspace of V is of dimension 2, and hence we may choose W so that $|g| = |g_1| \geq |g_2|$. So, we may assume $m > 1$. As $\phi_1(g_1)$ is cyclic, $g_1 = g|_W$ is orthogonally indecomposable on W , and $|g_1|$ is a p -power, it follows from Lemma 5.5 that $\langle g_1, Z(G_1) \rangle$ is of order $q^m \pm 1$.

Suppose first that $p > 2$. Then $|g_1| = (q^m \pm 1)/2$. As W is chosen of maximum dimension, we again get $|g| = |g_1| \geq |g_2|$. Recall that ϕ_1 is an irreducible Weil F -representation of G_1 (Lemma 5.1), and hence has dimension $(q^m - 1)/2$ or $(q^m + 1)/2$. As the matrix of $\phi_1(g_1)$ is cyclic, it has size $k = |g_1|$ or $|g_1| - 1$, and is similar to $\text{diag}(\varepsilon_1, \dots, \varepsilon_k)$, where the ε_i 's are pairwise distinct $|g_1|$ -roots of unity. On the other hand, $\phi(g) = \phi_1(g_1) \otimes \phi_2(g_2)$ has order at most $|g| \leq k + 1$. As $\phi(g)$ is almost cyclic, this contradicts Lemma 2.2 (unless $m = 1$, which is not the case here).

Next, let $p = 2$ (and hence $\ell \neq 2$ by (i)). Then $|g_1| = q^m \pm 1$ is a 2-power. As $m > 1$, in view of Lemma 2.6 this implies that $q^m = 3^2$, $|g_1| = 8$, $G_1 = Sp(4, 3)$ and $G = Sp(2n, 3)$. Let $t = g_1^4$ and $h = g^4$. Then $t = -\text{Id}$ and $h = \text{diag}(t, t')$, where $t' = g_2^4$. Note that, as $\phi_1(g_1)$ is cyclic, we have $\dim \phi_1 = 4$ by Lemma 4.15; in turn, this implies that $\phi_1(t) = -\text{Id}$.

Suppose first that $n > 3$. Then $\dim \phi_2 \geq (3^2 - 1)/2 = 4$. By Lemma 2.2 (as $\phi_1(g_1), \phi_2(g_2)$ are cyclic), we have $\deg \phi(g) \geq 4^2 - 4 + 1 = 13$, which is false as $|g| = |g_1| = 8$. Let $n = 3$. Then $G_2 = Sp(2, 3)$ is solvable, which is false. This completes the proof of the Proposition.

Proposition 5.13. *Let $SL(n, q) \subseteq G \subseteq GL(n, q)$, where $n > 2$ and $(n, q) \neq (4, 2), (3, 3)$ or $(4, 3)$. Let ϕ be an irreducible Weil F -representation of G , with $\dim \phi > 1$, and let $g \in G$ be a non-scalar semisimple element of prime-power order p^a for some prime p . Then $\phi(g)$ is almost cyclic if and only if g is irreducible and $|\langle g, Z(GL(n, q)) \rangle| = q^n - 1$.*

Proof. Observe first that the 'if' part of the statement follows from Lemma 4.11 and Corollary 5.3 (recall that, as $n > 2$, the irreducible Weil F -representations of G extend to $GL(n, q)$). So, from now on, we assume that $\phi(g)$ is almost cyclic.

Let V be the natural G -module, and let $W \subseteq V$ be a g -stable subspace of V on which g acts irreducibly, and such that $|g|$ coincides with the order of $g|_W$ (observe that this choice is possible as $|g|$ is a prime-power).

If $V = W$, then the statement follows from Lemma 5.5. Otherwise, by Lemma 4.12, g stabilizes no one-dimensional subspace (and hence also no subspace of codimension 1, by Maschke's theorem). Therefore, setting $\dim W = d$, we have $n - 1 > d > 1$ (so $n > 3$). Also, $|g|$ does not divide $q - 1$ (otherwise $g|_W$ would be scalar). Furthermore, we may assume that $(d, q) \neq (2, 2), (2, 3)$. (Indeed, if $(d, q) = (2, 2)$ then, since $(n, q) \neq (4, 2)$, we have $n \geq 5$. Then G is generated by at most n conjugates of g (by Proposition 2.9). As $\phi(g)$ is almost cyclic, and $|g| = |g|_W = 3$, we have $\dim \phi \leq 2n$ (by Lemma 2.11). However, the lower bound for $\dim \phi$ is $2^n - n - 1 > 2n$ for $n \geq 5$ (see [38]), which is a contradiction.

If $(d, q) = (2, 3)$, then $|g| = |g|_W \leq 8$, and hence V is the direct sum of 2-dimensional g -stable subspaces. It follows that g stabilizes a direct sum of subspaces $W' \oplus W''$, where $\dim W' = 4$, $g|_{W'} \neq \text{Id}$ and $\dim W'' = n - 4$. Then the claim follows from Lemma 4.14 for $(n, q) = (4, 3)$.

Now, we can write $V = W \oplus V'$, where V' is a g -stable subspace of V . Set $X = \{x \in SL(V) : x|_{V'} = \text{Id}\}$ and $Y = \langle X, g \rangle$. Clearly, $X \cong SL(W)$. Let $g_1 = \text{diag}(g|_W, \text{Id})$ and $g_2 = gg_1^{-1}$ (note that g_1, g_2 may not belong to G , but $|g_1| = |g|$). Set $Y_1 = \langle X, g_1 \rangle$. Then $Y \subset \langle Y, g_2 \rangle = Y_1 \times \langle g_2 \rangle$.

Let τ be any irreducible constituent of $\phi|_Y$. Then, by our assumption on $\phi(g)$, $\tau(g)$ is almost cyclic. Since g_2 centralizes Y , τ extends to a representation τ' , say, of $\langle Y, g_2 \rangle$. As $\tau'(g_2)$ is scalar and $g_1 = gg_2^{-1}$, the matrix of $\tau'(g_1)$ is almost cyclic. As $Y_1 = \langle X, g_1 \rangle$, one observes that $\tau'(Y_1)$ contains an almost cyclic matrix $\tau'(g_1)$. Set $X_1 = Y_1|_W \cong Y_1$. Then we can view $\tau'|_{Y_1}$ as a representation of X_1 . Note that $SL(W) \subset X_1 \subset GL(W)$. By Lemma 5.1, $\tau'|_X = \tau|_X$ is a Weil representation of X , and hence so is $\tau'|_{X_1}$.

Therefore, we can apply results obtained earlier to $\tau'(X_1)$. Namely, by Lemma 5.2(2), Lemma 5.7, Lemma 5.5 and the remark following it, it follows that either $d = 2$, or d is an odd prime and g_1 is a multiple of $(q^d - 1)/(q - 1)$, which must be a p -power. Moreover, if $d = 2$, then the order of g_1 must divide $2(q + 1)$, as g stabilizes no line on V .

Suppose first that $d > 2$, or $d = 2$ and p is odd. In this case, p is coprime to $q - 1$ (otherwise, by Zsigmondy's theorem, $(q^d - 1)$ would be divisible by a prime different from p). It follows that $\det g_1 = 1 = \det g_2$, and hence g is contained in $H := X \times X_2$, where $X \cong SL(W)$ and $X_2 \cong SL(V')$. As $(d, q) \neq (2, 2), (2, 3)$, by [47, Corollary 3.8], $\phi|_H$ contains an irreducible constituent τ that is non-trivial on both X and X_2 . Let $\tau = \tau_1 \otimes \tau_2$, where $\tau_1 \in \text{Irr}(X)$ and $\tau_2 \in \text{Irr}(X_2)$. Note that $\dim \tau_2 > 1$ unless $q = 2, 3$ and $n - d = 2$.

We need to examine the following cases:

(a) $d > 2$, $(n - d, q) \neq (2, 2), (2, 3)$. In this case we may apply Lemma 5.5 to g_1 . Namely, by Lemma 5.5 and Corollary 5.3, $\deg \tau_1(g_1) \geq |g_1| - 1$. Recall that g_2 is not scalar, as g stabilizes no one-dimensional subspace, and hence, as $SL(V')$ is quasi-simple, $\tau_2(g_2)$ is not scalar. Therefore, $\deg \tau(g) = \deg(\tau_1(g_1) \otimes \tau_2(g_2)) = |g|$. Note that the mappings $g \rightarrow \tau_i(g_i)$, $i = 1, 2$, yield representations of the group $\langle g \rangle$. If $p \neq \ell$, then $\tau(g)$ is not almost cyclic by Lemma 2.3. So, let $p = \ell$. Then, by Lemma 2.4, $\tau(g)$ is not almost cyclic unless $\ell \neq 2$ and $\dim \tau_1 = \dim \tau_2 = 2$. However, this implies $d = 2$, which is not the case.

Next suppose that $d > 2$, $(n - d, q) \in \{(2, 2), (2, 3)\}$. As p is coprime to $q - 1$ and $|GL(2, 3)| = 48$, the case $q = 3$ is ruled out. So, let $q = 2$. Note that g_2 is irreducible in $GL(n - d, q) = GL(2, q)$, as g stabilizes no line of V . As $\tau_1(g_1)$ is almost cyclic and τ_1 is a Weil representation of X , we have $|g_1| = 2^{n-2} - 1$ by Lemmas 5.5 and 5.7. As g_1 is irreducible on W , the eigenvalues of g_1 in $GL(n - 2, \overline{F}_2)$ are pairwise distinct primitive $|g_1|$ -roots of unity (by Galois theory), whereas the eigenvalues of g_2 in $GL(2, \overline{F}_2)$ are distinct primitive $|g_2|$ -roots of unity. Therefore, all the eigenvalues of g in $GL(n, \overline{F}_2)$ are pairwise distinct, unless $|g_2| = |g_1|$. In the latter case $d = n - 2 = 2$, which is not the case.

Thus, the eigenvalues of g in $GL(n, \overline{F}_2)$ are distinct, that is, g is a regular semisimple element and $C_G(g)$ has no unipotent element. By Lemma 2.8, G is generated by three conjugates of g . As $\phi(g)$ is almost cyclic and $\deg \phi(g) \leq |g|$, by Lemma 2.11, $\dim \phi \leq 3|g| - 3$. As $|g| = |g_1| = 2^{n-2} - 1$, we have $\dim \phi \leq 6(2^{n-3} - 1)$. On the other hand, the dimension of an irreducible F -representation of G is at least $2^{n-1} - n - 1$. This gives us a contradiction.

(b) $d = 2$, $p > 2$, $n \geq 4$. As p is odd here, $|g| \leq q + 1$, and G is generated by at most n conjugates of g (see Propositions 2.9 and 2.10). Then $\dim \phi \leq nq$, whereas $\dim \phi \geq (q^n - 1)/(q - 1) - 2$ as ϕ is a Weil representation. This is a contradiction.

(c) $d = p = 2$, $n \geq 4$. Then $|g| \leq 2(q + 1)$ and hence $\dim \phi \leq n(2q + 1)$, whereas $\dim \phi \geq (q^n - 1)/(q - 1) - 2$. This implies $q = 2$, and hence $p > 2$, a contradiction.

6. PROOF OF THEOREM 1.1

At this stage we are in a position to prove Theorem 1.1.

Proof of Theorem 1.1: Suppose first that $G = Sp(2n, q)$, $G \neq Sp(4, 3)$. Then $\tau(g)$ cannot be almost cyclic unless g is orthogonally indecomposable, by Proposition 5.12. So, assume that g is orthogonally indecomposable. Assume first that g is either a Singer or a Singer-type cycle. These cases are ruled out in Lemma 5.6, items (1) and (2) respectively, applying Lemma 2.6. So, assume that $|g|$ is a proper divisor of $q^n + 1$, $q^n - 1$, respectively. Then the claims (a) and (b) in item (1) of the statement follow from Lemma 5.7. Next, suppose that $G = Sp(4, 3)$. This group is dealt with in Lemma 4.15, yielding the cases under (c) in item (1) of the statement.

Now, suppose that $SU(n, q) \subseteq G \subseteq U(n, q)$, where $n > 2$ and $(n, q) \neq (5, 2), (4, 2), (3, 3), (3, 2)$. Remember that $|g|$ is assumed to be a prime-power, and recall the Remark following Lemma 5.5. Take into account Lemma 5.2, Corollary 5.3 and Lemma 5.7. Then claim (2),(a) of the statement follows from Lemma 5.11. Now, let us consider the 'exceptional cases' $(n, q) = (5, 2), (4, 2), (3, 3), (3, 2)$. The case $(n, q) = (5, 2)$ is dealt with in Lemma 4.17, yielding item (2),(b) of the statement. Next, suppose that $(n, q) = (4, 2)$. Observe that we may assume that $G = SU(4, 2)$. Then the claims in item (2),(c) of the statement follow from Lemma 4.16. Now, suppose that $(n, q) = (3, 3)$. If g is orthogonally indecomposable, then Lemma 5.2 and Lemma 5.7 yield $|g| = 7$. Otherwise g is orthogonally decomposable, and Lemma 5.9 applies. So the claims in item (2),(d) of the statement hold. Finally, suppose that $(n, q) = (3, 2)$. This case has been handled in detail by direct computation (see the Remark following Lemma 5.7), yielding item (2),(e) of the statement.

We are left with the case where $SL(n, q) \subseteq G \subseteq GL(n, q)$, with $n > 2$. Suppose first that $(n, q) \notin \{(3, 3), (4, 3), (4, 2)\}$. It then follows from Proposition 5.13 that $\tau(g)$ is almost cyclic if and only if g is irreducible and $|\langle g, Z(GL(n, q)) \rangle| = q^n - 1$. This yields items (3),(a) and (3),(b) of the statement, according to Lemma 5.2 and Lemma 5.7. Now, suppose that $(n, q) = (3, 3)$. This case is dealt with in Lemma 4.13, which gives $|g| = 13$, that is an instance of item (3),(b) of the statement. Next, suppose that $(n, q) = (4, 3)$. Then $\tau(g)$ is not almost cyclic, by Lemma 4.14. Finally, observe that the case $(n, q) = (4, 2)$ is ruled out by Lemma 4.11, (2), as we are assuming that τ is Weil, and hence has degree > 7 .

ACKNOWLEDGEMENT. We wish to thank Marco Antonio Pellegrini for having helped us with his skills in the use of the MAGMA and GAP packages for dealing with character tables and Brauer character tables, and for having provided efficient ad hoc routines for testing cyclicity and almost cyclicity of matrices.

REFERENCES

- [1] M. Aschbacher, *Finite group theory*, Cambridge University Press, Cambridge, 1986.
- [2] H.I. Blau, On linear groups with a cyclic or TI-Sylow p -subgroup, *J. Algebra* 114(1988), 268 - 285.
- [3] C. Bonnafé, *The representations of $SL_2(\mathbb{F}_q)$* , Springer-Verlag, Heidelberg, 2011.
- [4] R. Burkhardt, Die Zerlegungsmatrizen der Gruppen $PSL(2, p^f)$, *J. Algebra* 40(1976), 75 - 96.
- [5] J. Conway, R. Curtis, S. Norton, R. Parker and R. Wilson, *Atlas of finite groups*, Clarendon Press, Oxford, 1985.
- [6] U. Dempwolff, Linear groups with large cyclic subgroups and translation planes, *Rend. Sem. Mat. Univ. Padova* 77(1987), 69 - 113.
- [7] L. Di Martino, M. A. Pellegrini and A.E. Zalesski, On generators and representations of the sporadic simple groups, *Comm. in Algebra*, 42:2 (2014), 880-908.
- [8] L. Di Martino and A.E. Zalesski, Minimum polynomials and lower bounds for eigenvalue multiplicities in representations of classical groups, *J. Algebra* 243(2001), 228-263. Corrigendum: *J. Algebra* 296(2006), 249 - 252.
- [9] L. Di Martino and A.E. Zalesski, Eigenvalues of unipotent elements in cross-characteristic representations of finite classical groups, *J. Algebra* 319(2008), 2668-2722.

- [10] L. Di Martino and A.E. Zalesski, Unipotent elements in representations of finite groups of Lie type, *J. Algebra and App.* 11(2) (2012), pp.1250038-1 – 1250038-25.
- [11] K. Doerk and T. Hawkes, *Finite soluble groups*, De Gruyter publ., Berlin, 1992.
- [12] N. Dummigan and Pham Huu Tiep, Lower bounds for minima of certain symplectic and unitary group lattices, *Amer. J. Math.* 121(1999), 889 – 918.
- [13] L. Emmett and A.E. Zalesski, On regular orbits of elements of classical groups in their permutation representations, *Comm. Algebra* 39:9 (2011), 3356 – 3409.
- [14] V. Ennola, On the characters of finite unitary groups, *Ann. Acad. Sci. Fenn. Ser. A, I*, 323(1963), 120 – 155.
- [15] W. Feit, *The representation theory of finite groups*. North-Holland, Amsterdam, 1982.
- [16] P. Gérardin, Weil representations associated to finite fields, *J. Algebra* 46(1977), 54 – 101.
- [17] R. Gow, Commutators in finite simple groups of Lie type, *Bull. London Math. Soc.* 32(2000), 311 – 315.
- [18] R. Guralnick and W. Kantor, Probabilistic generation of finite simple groups, *J. Algebra* 234(2000), 743 – 792.
- [19] R. Guralnick, T. Penttila, C. Praeger and J. Saxl, Linear groups having certain large prime divisors, *Proc. London Math. Soc.* (3) 78(1999), 167 – 214.
- [20] R. Guralnick and J. Saxl, Generation of finite almost simple groups by conjugates, *J. Algebra* 268(2003), 519 – 571.
- [21] Ch. Hering, Transitive linear groups and linear groups which contain irreducible subgroups of prime order. I. *Geom. Dedicata* 2(1974), 425-460.
- [22] Ch. Hering, Transitive linear groups and linear groups which contain irreducible subgroups of prime order.II. *J. Algebra* 93(1985) (1), 151-164.
- [23] G. Hiss and G. Malle, Low-dimensional representations of special unitary groupss, *J. Algebra* 236(2001), 745 – 767.
- [24] G. Hiss and A. Zalesski, The Weil-Steinberg character of finite classical groups with an appendix by Olivier Brunat, *Represent. Theory* 13(2009), 427-459.
- [25] W.C. Huffman and D.B. Wales, Linear groups containing an element with an eigenspace of codimension two. Proceedings of the Conference on Finite Groups (Univ. Utah, Park City, Utah, 1975), pp. 425–429. Academic Press, New York, 1976.
- [26] B. Huppert, *Character theory of finite groups*, De Gruyter publ., Berlin, 1998
- [27] B. Huppert, Singer-Zyklen in klassischen Gruppen, *Math. Z.* 117(1970), 141-150.
- [28] B. Huppert and N. Blackburn, *Finite groups II*, Springer-Verlag, Berlin etc., 1982.
- [29] C. Jansen, K.Lux, R. Parker and R. Wilson, *An Atlas of Brauer characters*, Oxford Science publications, Clarendon Press, Oxford, 1995.
- [30] P. Kleidman and M. Liebeck, *The Subgroup Structure of the Finite Classical Groups*. Cambridge Univ. Press, Cambridge, 1990. (London Math. Soc. Lecture notes no.129.)
- [31] V. Landazuri and G. Seitz, On the minimal degrees of projective representations of of the finite Chevalley groups, *J. Algebra* 32(1974), 418 – 443.
- [32] F. Lübeck and G. Malle, (2,3)-generation of exceptional groups, *J. London Math. Soc.* 59(1999), 109 – 122.
- [33] G. Malle, Hurwitz groups and $G_2(q)$, *Canad. Math. Bull.* 33(3)(1990), 349 – 356.
- [34] G. Malle, Small rank exceptional Hurwitz groups, In: *Groups of Lie type and their geometries*, London Math. Soc. Lecture Notes vol. 207, Cambridge Univ. Press, Cambridge, 1995, 173–183.
- [35] G. Malle, J. Saxl and Th. Weigel, Generation of classical groups, *Geom. Dedicata* 49(1994), 85 – 116.
- [36] H. Pollatsek, Irreducible groups generated by transvections over finite fields of characteristic two. *J. Algebra* 39 (1976), 328 – 333.
- [37] Ch. Rudloff and A.E. Zalesski, Regular submodules for cyclic Sylow p -subgroups in complex representations of classical groups, *J. Group theory* 10(2007), 585 – 612.
- [38] G. Seitz and A.E. Zalesskii, On the minimal degrees of projective representations of the finite Chevalley groups, II, *J. Algebra* 158(1993), 233-243.
- [39] J.-P. Serre, *Linear representations of finite groups*, Springer-Verlag, Hiedelberg, 1977.
- [40] A. Stein, $1\frac{1}{2}$ -generation of finite simple groups, *Beiträge Algebra Geom.* 39(1998), 349 – 358.
- [41] I.D. Suprunenko, Unipotent elements of non-prime order in representations of the classical algebraic groups: two big Jordan blocks, *Zapiski Nauch. Semin. POMI* 414 (2013), 193 – 241.
- [42] I.D. Suprunenko and A.E. Zalesski, Irreducible representations of finite classical groups containing matrices with simple spectra, *Comm. Algebra* 26(1998), 863 – 888.
- [43] I.D. Suprunenko and A.E. Zalesski, Irreducible representations of finite groups of exceptional Lie type containing matrices with simple spectra. *Comm. Algebra* 28(2000), no.4, 1789–1833.
- [44] M. Suzuki, *Group theory I*, Springer-Verlag, Berlin, 1982.
- [45] Pham Huu Tiep and A.E. Zalesskii, Some characterizations of the Weil representations of the symplectic and unitary groups, *J. Algebra* 192(1997), 130-165.

- [46] Pham Huu Tiep and A.E. Zalesskii, Some aspects of finite linear groups: A survey, *J. Math. Sciences* Vol. 100(2000), 1893-1914. (Russian edition: *Contemporary Mathematics and its Applications. Thematic Surveys*. Vol. 58, Algebra - 12.)
- [47] Pham Huu Tiep and A.E. Zalesski, Hall-Higman type theorems for semisimple elements of finite classical groups, *Proc. London Math. Soc.* (3) 97(2008), 623 - 668.
- [48] A. Wagner, Determination of the finite primitive reflection groups over an arbitrary field of characteristic not two, Parts I, II, III, *Geom. Dedicata* 9(1980), 239 - 253, 10(1981), 191 - 203, 475 - 523.
- [49] A. Wagner, Collineation groups generated by homologies of order greater than 2, *Geom. Dedicata* 7(1978), 387 - 398.
- [50] H.N. Ward, Representations of symplectic groups, *J. Algebra* 20(1972), 182 - 195.
- [51] A.E. Zalesskii, The normalizer of the extraspecial linear group (in Russian). *Vesti AN BSSR, ser. fiz.-mat. nauk* 1985, no.6, 11 - 16.
- [52] A. Zalesski, Spectra of elements of order p in representations of Chevalley groups of characteristic p (in Russian). *Vesti AN BSSR, ser. fiz.-mat. nauk* 1986, no.6, 20 - 25.
- [53] A.E. Zalesskii, Linear groups. In: *"Encyclopedia of Mathematical Sciences", vol.37: Algebra IV*, Springer-Verlag, Berlin, 1993, 97 - 196.
- [54] A.E. Zalesskii, Minimal polynomials and eigenvalues of p -elements in representations of groups with a cyclic Sylow p -subgroup, *J. London Math. Soc.* 59(1999), 845 -866.
- [55] A.E. Zalesski, The number of distinct eigenvalues of elements in finite linear groups, *J. London Math. Soc.* Part 2, 74(2006), 361 - 378.
- [56] A.E. Zalesski, Minimal polynomials of the elements of prime order in complex irreducible representations of quasi-simple groups, *J. Algebra* 320(2008), 2496 - 2525.
- [57] A.E. Zalesski, On eigenvalues of group elements in representations of simple algebraic groups and finite Chevalley groups, *Acta Applicanda Mathematicae* 108(2009), 175 - 195.
- [58] A.E. Zalesskii and V.N. Serezhkin, Linear groups generated by transvections. *Math. USSR, Izvestija* 10(1976), 25 - 46.
- [59] A.E. Zalesskii and V.N. Serezhkin, Linear groups generated by reflections, *Math. USSR, Izvestija*, 17(1981), 477 - 503.
- [60] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. für Math. Phys.* 3(1892), 265 - 284.

Authors' addresses: Dipartimento di Matematica e Applicazioni, Università degli Studi di Milano-Bicocca, Via R. Cozzi 53, Milano, 20125, Italy
e-mail: lino.dimartino@unimib.it, alexandre.zalesskii@gmail.com